Bioinspired Immune System for Intrusions Detection System in Self Configurable Networks

Noor Mohd[*,1], Annapurna Singh[2], H.S. Bhadauria[3]
Computer Science and Engineering, G. B. Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand (India)[1]
Computer Science and Engineering, Graphic Era Deemd to be University, Dehradun, Uttarakhand, (India)[1]
Computer Science and Engineering, G. B. Pant Institute of Engineering and Technology
Pauri Garhwal, Uttarakhand (India)[2, 3]

***Abstract*—In the last couple of years, the computer frameworks have become more vulnerable to external attacks. The PC security has become the prime cause of concern for every organization. To achieve this objective Intrusion Detection System (IDS) in self-configurable networks has played a vital role in the last few decades to guard LANs. In this work, an IDS in self-configurable networks is deployed based on Bioinspired Immune System. IDS in self-configurable networks are accustomed to monitor data and network activity and alert when any suspicious activity observed security heads are alerted. A vital and common application space for versatile frameworks swarm-based is that of PC security. A PC security framework ought to protect a machine or accumulation of machines from unapproved gatecrashers. The framework seems to be capable of counteracting against external activity. Also it is comparable in usefulness to secure framework shielding from intrusion by external threats like in case of attacking microorganisms. A counterfeit insusceptible framework is a PC programming framework that mirrors a few sections of the conduct of the human resistant framework to shield PC systems from infections and comparable digital assaults. This paper demonstrates the need of a novice substring seeks calculation based on bio-roused calculations. Tests are required to create system for Network Intrusion detection that aids in securing a machine or clusters of machines from unapproved intruders. In this paper IDS in self-configurable networks is implemented by using Bio-inspired Immune System and KMP algorithm as a model IDS.**

Keywords—Networks security; intrusion detection system; AIS algorithm; KMP algorithm; self-configurable networks

I. Introduction

With the automation of computational processes and involvement of personal computer in daily life is needed to be additionally smart and more secure to active as well as passive attacks. It has been also noted that the PC are more and more exposed to assaults, because of its broad range web accessibility. For this reason PC security has become the fundamental cause of worry for developing IDS. Interruptions cause calamity inside LANs and the time and cost to assess and comeback the damage could be immense.

Interruption Detection Arrangements (IDA) [1] are used to observed information concerning them and depicting them to security heads.

An indispensable and normal demand territory for versatile courses of action swarm built up is that of PC security. A computer protection arrangement such as Web Intrusion detection Arrangement should prevent a contraption or assembly of mechanisms from unauthorized intruders. The arrangement ought to additionally be able stop opposing an external program that is comparable in functionality with the immune arrangement protecting itself from conquest by microbes. An Artificial Immune Arrangement (AIS) [2] is a computer multimedia arrangement that depicts little parts of the action in case of human immune arrangement. It protects computer webs from harmful viruses in addition to comparable cyber-attacks.

A. *Intrusion Detection System*

Interruption discovery is the full components for observing the different type of incident that happened in PC framework environment. The system investigates for signs of various contravention or dangers of breaching PC security methodologies, suitable utilized approaches, or normal security hone. Threats to PC systems are extending because of increased used of internet and local region systems [3, 5, 14, 16, 17 and 18]. Laptops are evolving so one can get more involved to fight automobile endemic network connectivity. They have been attacking work targets of many malicious threats that invariably morph into actual intrusions. This is often what’s causing its computer security in a dynamic concern for the network. Intrusions may lead to adverse effects on LANs in addition to the wasted time price to renovate the destruction can grow to great proportions. As an alternative employing passive measures automobile and patch security hole once and will be exploited, it may appear far more proficient to get a proactive measure to intrusions. IDS in self-configurable networks are widely accepted and used to monitor the facts about them, also reporting the crooks to security administrators.

The fundamental model of IDS in self-configurable networks demonstrated in Fig. 1 is consisting of a data collection section, detection rule section and response section.

Intrusion Detection Systems support various type of information systems plan for, and treat with attacks. They do this by collecting related information from various types of systems and network sources and then analyzing the results for occurring possible security problems.

*Corresponding Author

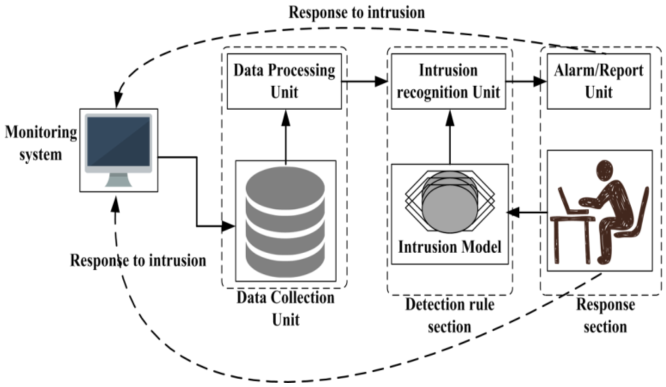


Fig. 1. Fundamental Model of Intrusion Detection System in Self Configurable Networks.

1) Monitoring and study of user behavior and system activity.

2) Defining the system configurations and susceptibilities?

3) Integrity access to important critical system and related data files.

4) The Statistical analysis of activity prototype using the signature-based matching attacks.

5) Irregular different type of activity analysis, Operating-system audit.

B. IDS Methodologies

Interruption discovery framework utilizes numerous procedures to make note of occurrences. Essentially IDPS advances utilize different discovery procedures, either discretely or incorporated, to allow more wide and precise location.

Signature Based Detection: A signature can be an example that compares with a known danger. Mark based discovery is components for divergent marks against inspected occasions with feasible occurrences. Mark based location could be exceptionally gripping at distinguishing known threats however, mostly insufficient at identifying beforehand doubtful threats [6].

Illustration: A contact with the principle theme of free pictures and connection filename of freepics.exe, these attributes shows known type of malware. On the off chance that assailants alter the document name freepics.exe to freepics1.exe, signature based recognition will battle to distinguish this malware.

Constraints: It wouldn't see already unidentified dangers.

Abnormality Based Detection: Abnormality based recognition is a task of contrasting meanings of what exercises is respected typical against watched occasions to perceive real deviations. IDPS utilizing change based recognition has profiles that speak to standard conduct of territories like a purchaser, has arranged associations or applications. The profile is delivered by observing and qualities of run of the mill exercises, an assortment of email send by the client, assortment of fizzled login endeavors for tons and the state of processor use for tons with a period of time. Oddity based recognition is very capable of identifying beforehand obscure dangers.

Confinements: Building profile is greatly testing

Stateful Protocol Analysis: Stateful convention investigation is a task of looking at foreordained profiles of by and large acknowledged the meanings of favorable agreement exercises for every agreement state against observed distances to perceive deviations. Stateful convention examination relies upon merchant created public profiles that determine the way of specific convention ought to and ought not to be utilized. The Stateful in Stateful convention analysis [9] implies the IDPS is ideal for comprehension and following the state of transport, system and application conventions that have a generally thought of state.

Constraints: It's restricted by looking at one single demand or reaction. Numerous assaults are not identified by survey one demand – the assault may include various solicitations.

The rest of paper is organized in the following manner. Section I is used to represent introduction about IDS and their respective methodologies. Section II is discussed about the techniques about IDS. The next section (Section III) is consisting of propose work and KMP string matching algorithm. The simulation and results are discussed in Section IV. Finally whole work is concluded in Section V and future scope of the proposed work has been described in Section VI.

II. Techniques of Intrusion Detection System

IDS in self-configurable networks uses as a few strategies, including the IDS halting the assault itself, altering the security condition (Like- reconfiguration a firewall), or changing the assault's substance. The types of IDS technologies [15] are separated principally by the sorts of occasions build by screen and also ways that they have been conveyed.

Network Behavior Analysis (NBA): This analyzes arrange guests distinguish dangers that produce uncommon movement streams, as dispersed refusal and administrations data assaults, such as assortments malware, and strategy infringement (e.g. an individual framework giving system administrations to systems). Behavior-Based Analysis [10] learns customary conduct of activity and frameworks at that point persistently looks at them for potentially harming oddities and with conduct that oftentimes go with episodes. This procedure distinguishes assaults by their business, rather their code matches strings found in a particular past episode. "It stops activity that is not malevolent all over but rather that will do noxious things", said by Allan Paller.

Remote Intrusion Recognition Framework: This strategy checks remote system movement. It anatomizes to differentiate doubtful action for the remote systems administration agreements themselves.

Host-Based Intrusion Location Framework: With the capacity to break down exercises relating for the host it screens quickly when contrasted and propelled a more elevated amount angle, it could quite every now and again pick which forms or potentially clients encounter malevolent exercises. When they may each concentration utilizing one host, have based IDS in self-configurable networks frameworks promptly operator comfort demonstrate where specialist run utilizing (and screen) singular has yet they are responsible to a specific unified reassure (so on the off chance that you experience the ill effects of an individual support can design, direct, and unite information from various hosts). Host-based IDSs can see assaults undetectable with your system based IDS in self-configurable networks and can check assault impacts precisely.

System Based Intrusion Location Framework: It inspects or screens an entire, incredible system with a not very many all-around arranged hubs or gadgets and forces minimal overhead on organize implement. It breaks the system and application agreement action to differentiate doubtful incidents. The system based IDSs in self-configurable networks are regularly detached gadgets that screen continuous system action without including huge overhead or aggravating system operation [13]. They're extremely all too simple to control assault and can be imperceptible to assailants; moreover, they merit giving little exertion and fit and utilize on existing systems. A sensor is sent in 1 of 2 modes inline mode and aloof mode.

Inline Mode: An inline sensor is conveyed so your system activity it happens to screen must go all through, much the same as the movement stream of a firewall. Personally, some inline sensors are half and half firewall/IDS gadgets, mortgage holders are essentially just IDSs. The main inspiration for arranging IDS in self-configurable networks sensors inline is ordinarily to help them to stop assaults by blocking system activity.

Detached Mode: A latent sensor is sent all together that it screens a copy of that system activity; no movement passes employing the sensor. Inactive sensors are normally sent with a specific end goal to screen key system areas, for example, the divisions amongst systems, and key system sections, similar to action even on a neutral territory (DMZ) subnet.

Problem Formulation: The inclusion in gazing at the resistant component is expanding over the past couple of years. PC researchers, engineers, mathematicians, thinkers alongside different scientists are especially intrigued with the capacities for this framework, whose unpredictability is practically identical to that of the cerebrum. An inventive area of research called Artificial Immune Systems has emerged [4, 7 and 12]; however no formal basic structure was introduced yet.

Numerous properties on the resistant instrument are engaging for PC researchers and specialists:

1) Uniqueness: Everyone has a particular invulnerable system, including its specific vulnerabilities and abilities.

2) Recognition of Nonnative: The (unsafe) molecules which are not indigenous to the body's cells are identified and eliminated within view of the insusceptible instrument.

3) Anomaly Location: The safe system can recognize and behave to pathogens that the body's cells have not experienced previously.

4) Distributed Discovery: The cells networks on the framework are circulated all around the body and, uncovered this as a main priority, aren't represented by any unified control.

5) Imperfect Location (Clamor Resilience): The correct acknowledgment on the pathogens isn't important; hereafter the hole is adaptable.

6) Reinforcement Learning and Memory: It can "take in" the structures of pathogens, to verify that future reactions with similar pathogens are quicker and more grounded.

The resistance instrument is greatly confounded and resembles it's correctly tuned with the issue of identifying and wiping out infections [8]. It's accepted since it likewise offers a convincing commendable instance of your dispersed data preparing framework, the person who we can consider for, to guarantee planning better artificial versatile frameworks.

A major and regular application area for versatile frameworks swarm-based is the one about PC security. Some kind of PC security measure such concerning case Network Intrusion identification System ought to ensure an instrument or wide assortment of machines from unapproved gatecrashers. These gadgets prerequisites find a route avoid against outside code that will be comparable in usefulness with the safe framework shielding the self from intrusion by microorganisms (quiet). Thus convincing similitude among the self and non-self codes, outline for this "counterfeit insusceptible framework". (AIS) may be ensuring PC systems dependent on safe legitimate standards, calculations and design. This proposition goes enhancing Naïve String Search calculation for used in artificial body; the entire Naive string looking calculation discovers all events related with a solitary given string inside another. These have running time multifaceted nature is corresponding with the volume of the lengths out of your strings in the altered calculation may potentially be stretched out to keep up considerably more broad example coordinating issues.

Fake insusceptibility framework is unquestionably programming applications framework that impersonates tune for the conduct out of your human resistance framework to shield PC systems from infections alongside other alike digital assaults. The first thought could be the human resistance framework, which is unquestionably a complicated framework involving lymphocytes.

In this work KMP String Search calculation is implemented with regards to illustration in c# environment for fake insusceptible framework. The Modified Generic KMP string looking calculation brings about lymphocyte in the swarm-based fake resistant framework. The authors are trying to compose a reproduction instrument encountering how AIS acts. All reproduction tests and mimicking programs are in the like manner written in the C# programming dialect or client Defined sources of info.

A noteworthy and regular application space for versatile frameworks swarm-based speaks to PC security. Your PS security such with regards to illustration Network Intrusion discovery System ought to ensure one device or measure of machines from unapproved interlopers. What's more, it needs to have the decision anticipate against outside code, which is proposed to be comparable in usefulness considering the invulnerability framework shielding the self from intrusion by microorganisms.

Thus convincing closeness among the self and non-self-codes, outline for this “Artificial Immune System” (AIS) [11 and 19] may be ensure PC systems dependent on invulnerable coherent standards, calculations and engineering. This proposition goes enhancing Naïve String Search calculation for use in artificial body; the entire Naive string looking calculation discovers all events related with a solitary given string inside another. These have running time intricacy is relative with the volume of the lengths out of your strings in the altered calculation may potentially be reached out to keep up much more broad example coordinating issues.

Fake insusceptibility framework is unquestionably programming applications framework that impersonates tune for the conduct out of your human invulnerability framework to shield PC systems from infections alongside other alike digital assaults. The first thought could be the human insusceptibility framework, which is certainly a many-sided framework containing lymphocytes.

III. Proposed Work

AIS for network intrusion detection are an automated system tot models some components of the behavior in the human immunity system. It aims to safeguard the computer networks from harmful viruses as well as other attacks like active or passive. Considering that the human immunity method is problematic system composed of lymphocytes, antibodies as well as other components have evolved and energy to will protect you against harmful pathogens. Hence, modeling the behavior in the human immunity system must provide a prospering method against attacks.

The major elements of a simplified immune system are illustrated in Fig. 2. It consisting of harmful nodes called antigens shown as red. The human body also contains many healthy antigens called self-antigens shown as green in Fig. 2 and some naturally occurring proteins are shown as rounded ovals.

A. *Implementation of AIS for Network Intrusion Detection Development*

For the development of a swarm-based system which is in particularly targeted towards Network Intrusion Detection in self-configurable networks, few key factors are considered like.

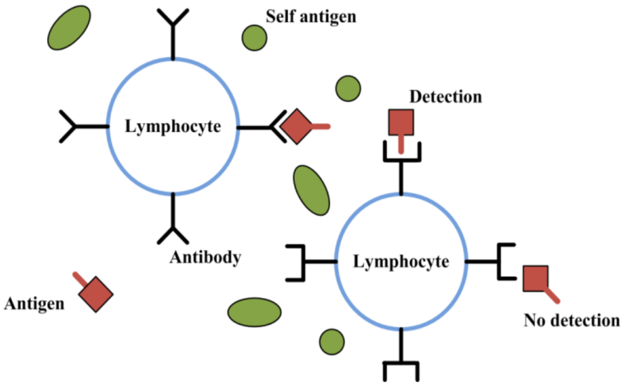


Fig. 2. Elements of IS.

- The safe framework ought to be assorted, which enormously enhances heartiness, on both a populace and individual level, for instance, extraordinary individuals are helpless against various organisms; in the event of systems the framework ought to have the capacity to recognize expansive IP swarm if there should be an occurrence of Denial of Service Attacks.
- It ought to be circulated, comprising of numerous segments that cooperate locally to give worldwide assurance, so there is no focal control and henceforth no single purpose of disappointment.
- It ought to be blunder tolerant in that a couple of missteps in grouping and reaction are not calamitous.
- It ought to be dynamic in nature, i.e. singular segments are persistently made, devastated, and are flowed all through the body, in the event of Network the framework ought to have the capacity to distinguish any kind of Addressed for instance Ipv4 or Ipv6 in any case.

B. *KMP Algorithm*

KMP Algorithm detects all circumstance of just one identified substring within another string, in dynamic manner corresponding to the actual length of the string. The proportionality constant is very small to produce given algorithm run practical, and hence the process is required to be further enlarging to manage even two or more basic pattern-matching problems. A conceptual application in this approach implies that the group of concatenations of even palindromes like the language could be accepts in linear time.

Text-editing programs are often requisition to search through a string of characters focus for occurrence of a given “pattern” string. In this work authors desire to find all type of positions, or perhaps only the leftmost position, in which the pattern occurs as a contiguous substring of the text. For example, “*Butterfly*” contains the pattern “*fly*”, but we do not regard “*Butterfly*” as a substring.

The decided way to search for a matching pattern is to try searching at every starting position of the text, leave the search as soon as an incorrect character is search. But in this approach can be very ineffective, for example when we are considering for an occurrence of aaaaaaab in aaaaaaaaaaaaaab.

When the given pattern is $a^n b$ and the text is $a^2 b$, we will find ourselves making $(n+1)$ comparisons of given characters. Furthermore, the conventional approach involves “backing up” the input text as we go through it, and this can add provoking complications when we consider the buffering operations that are usually involved.

However KMP Algorithm finds all occurrences of a routine of length ***m*** in just a text of length ***n***. Time Complexity of KMP algorithm is

$$O(m+n) \tag{1}$$

The algorithm needs only $O(m)$ locations of internal memory if the writing is read from an additional file, and only $O(\log m)$ units of time elapse between consecutive single-character inputs. All the constants of proportionality implied by these "O" formulas are independent of the alphabet size.

C. Working of KMP Algorithm

The working of KMP algorithm is given as

Step 1: Initialize the input variables:
n = Amount for the Text, m = Amount for the Pattern,
u = Prefix –function of pattern (p) and
q = Lots of characters matched.

Step 2: Define the variable: q=0, the start of match.

Step 3: Compare initial character for the pattern with first character of text. If the match isn't found, substitute the worthiness of u[q] to q. If the match can be found at, then increment the worthiness of q by 1.

Step 4: Check whether lots of the pattern elements are matched considering the writing elements. Or simply, repeat the search process. If yes, print the level of shifts taken via the pattern.

Step 5: Often search for another match.

D. Modified KMP Algorithm for a Lymphocyte

The Lymphocyte Detects uses the Knuth-Morris-Pratt substring algorithm that may be affixed to any Pieces of an IP Address. The KMP algorithm Detects accepts a look pattern such a few instance 1010100 and returns true if the present object's antigen, such a few instance 101, matches the pattern.

Algorithm

The modified KMP algorithm for proposed IDS in self-configurable networks is given as

```
Initialize the parameters
$n \leftarrow length[\mathrm{S}];\ m \leftarrow length[\mathrm{p}];$
$a \leftarrow compute\,\mathrm{Pr}\,efixFunction;\ q \leftarrow 0;$
                    for $i \leftarrow 1$ to $n$ do
while $q \geq 0$ and $p[q+1]$,
$S[i]$ do // S is the gene search table
$q \leftarrow a[\mathrm{p}]$ // p is the Incoming Gene Pattern
  if $p[q+1] = \mathrm{S[i]}$ // Match Pattern in the gene database
then
$q \leftarrow q+1$
end if;
if $q == m$ then
$q \leftarrow a[q]$     // The Gene Pattern is Detected
   end if;
end while;
end for;
```

IV. Simulation and Results

The working flow chart of the designed IDS in self-configurable networks is given in Fig. 3.

The simulation parameters opted for this work is listed in Table I. From the Table I, it has been observed that virus gene size is equal to 32 and antibody size is 10 considered for this simulation. The used threshold value for this experiment is 3, swarm size is 10. The maximum age of virus is 10 and maximum simulation count is 1000 considered for this experiment.

The performance of the developed IDS in self-configurable networks system has been evaluated by the help of optimal number of Lymphocyte for Ipv4 packets, Ipv4 detection time vs. number of Lymphocytes and simulation time.

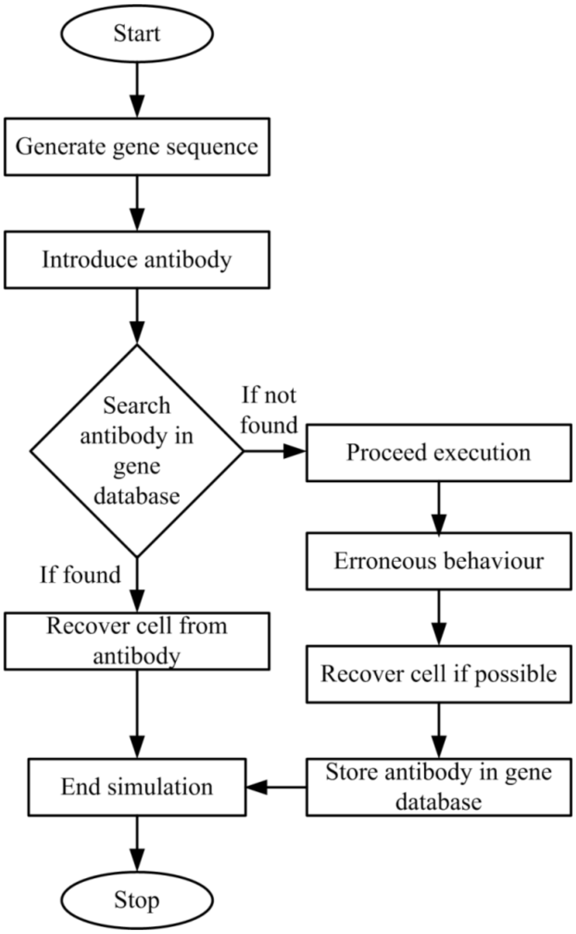


Fig. 3. Working flow Chart of the Proposed Work.

TABLE. I. Simulation Parameters

Parameter Name	Value
Virus Gene Size	32
Anti Body Size	10
Threshold	3
Swarm Size	10
Max Age	10
Simulation Count	1000

A. Simulation Results

The optimal number of Lymphocyte for Ipv4 Packets and average detection time are given in Table II for above said simulation parameters. The graphical representation of results is shown in Fig. 4.

From the Table II and Fig. 4, it has been observed that optimal number of Lymphocytes is 14 and average detection time is 1.4 milliseconds.

Further, the developed IDS in self-configurable networks have been repeatedly simulated in same environment using artificial immunity simulator as per shown in Fig. 5.

The simulation time results of Ipv4 simulation for various simulation counts have been reported in Table III and also shown in Fig. 6.

TABLE. II. IPV4 DETECTION TIME VS. NO OF LYMPHOCYTES

No of Lymphocytes	Ipv4 Detection Time(AVG)
1	0.51
2	0.68
3	0.70
4	0.85
5	0.88
6	1.06
7	1.21
8	1.41
9	1.60
10	1.77
11	1.79
12	1.45
13	1.41
14	1.41
15	1.43
16	1.41
17	1.42
18	1.41
20	1.41

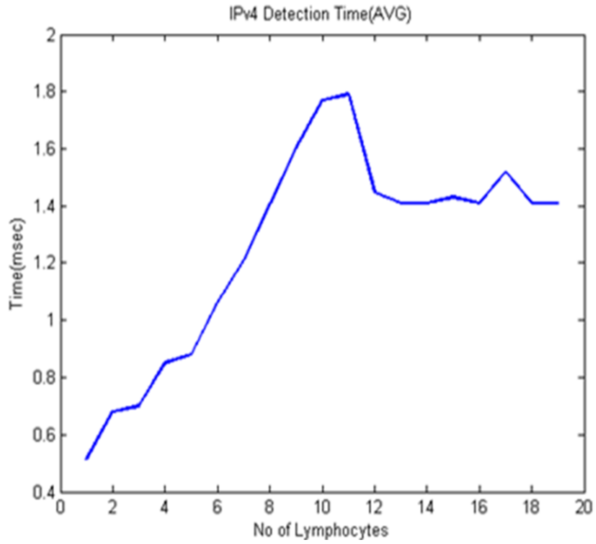
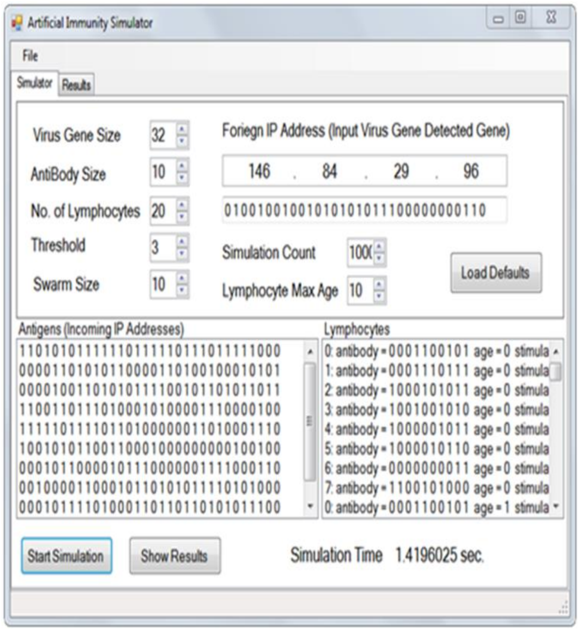


Fig. 4. Ipv4 Detection Time vs. No of Lymphocytes.



Virus Gene Size 32

AntiBody Size 10

No. of Lymphocytes 20

Threshold 3

Swarm Size 10

Foriegn IP Address (Input Virus Gene Detected Gene)

146 . 84 . 29 . 96

01001001001010101011100000000110

Simulation Count 100(

Lymphocyte Max Age 10

Antigens (Incoming IP Addresses)

```
11010101111110111110111011111000
00001101010110000110100100010101
00001001101010111100101101011011
11001101110100010100001110000100
11111011110110100000011010001110
10010101100110001000000000100100
00010110000101110000001111000110
00100001100010110101011110101000
00010111101000110110110101011100
```

Lymphocytes

```
0: antibody = 0001100101 age = 0 stimula
1: antibody = 0001110111 age = 0 stimula
2: antibody = 1000101011 age = 0 stimula
3: antibody = 1001001010 age = 0 stimula
4: antibody = 1000001011 age = 0 stimula
5: antibody = 1000010110 age = 0 stimula
6: antibody = 0000000011 age = 0 stimula
7: antibody = 1100101000 age = 0 stimula
0: antibody = 0001100101 age = 1 stimula
```

Simulation Time 1.4196025 sec.

Fig. 5. Artificial Immunity Simulator.

TABLE. III. IPV4 SIMULATION TIME

Simulation Count	Simulation Time
100	0.0811
200	0.1286
300	0.1794
400	0.2246
500	0.2808
600	0.3274
700	0.3665
800	0.4289
900	0.4782
1000	0.5147

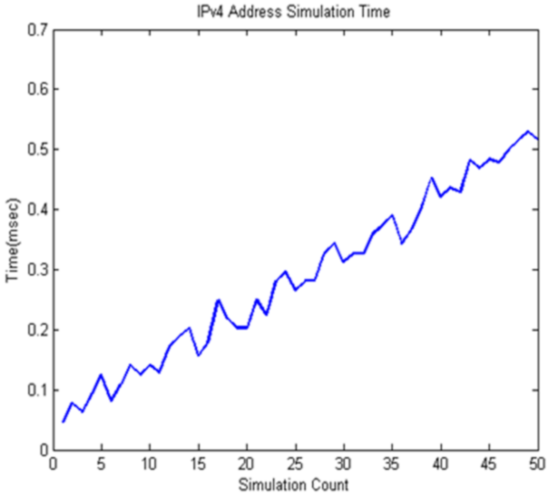


Fig. 6. Graph Showing Ipv4 Simulation Time.

B. Comparative Analysis

The present work is compared with the study performed by Belouch [16] in terms of simulation time. It is worth to mention that the minimum simulation time for 100 nodes is 0.08 seconds. The total simulation time for study performed in study [16] is 0.20 seconds. Therefore, it has been observed that the IDS based on KMP string matching and AIS based system is more fast that machine learning based system.

V. Conclusion

The insusceptibility procedure is considered that conveys both guard and upkeep inside the body. Numerous reasons exist why the insusceptibility procedure is surely seen as path for you to motivation for any plan of novel calculations and frameworks. This proposition concerned utilizing Naïve String Search calculation for used for counterfeit resistance process; the aggregate Naïve string looking calculation discovers all events of a specific string inside another. You can discover running time multifaceted nature is corresponding to measure of one's lengths inside the strings also; the adjusted calculation can be stretched out to hold other general example coordinating issues.

We created Algorithms that were bio motivated and given reenactments to Network interruption recognition situations. The Algorithm utilized the versatile credulous string look calculation as Pattern Matching calculation to copy the conduct of a man or lady Lymphocyte. The calculation gave fruitful and fulfilling the results.

VI. Future Scope

A swarm-based artificial invulnerable algorithm is among numerous calculations enlivened by natural frameworks, including developmental calculations, swarm knowledge, neural systems and layer processing. AIS are naturally enlivened calculations that take their motivation from a human or creature resistant framework. Inside AIS, classes of sorts of calculations, and principals are centered chiefly at the speculations of invulnerable systems including, clonal choice and negative choice. These hypotheses have just been consolidated into different calculations and been given wear various application territories.

In any case, necessary and normal application space for versatile frameworks swarm-based is PC security. Your working PC framework security including Network Intrusion recognition System ought to ensure a PC gadget or few machines from unapproved interlopers. The sewing machine ought to in like manner give you the possibility averts against outside code that is similar in usefulness to insusceptibility process shielding the self from attack by organisms (non-self).

We can readily see following areas are suitable in the foreseeable future:

1) Improve Lymphocyte performance for Ipv4 and particularly Ipv6 Networks.

2) Capability auto load Network addressed into cache for faster detection.

3) Improved clone selection and negative selection.

4) Using Devised Methodologies for coming of spam detection framework and actual implementation of AIS algorithms for spam Detection.

References

[1] Casas, P., Mazel, J., & Owezarski, P. (2012). Unsupervised network intrusion detection systems: Detecting the unknown without knowledge. Computer Communications, 35(7), 772-783.

[2] Dasgupta, D. (Ed.). (2012). Artificial immune systems and their applications. Springer Science & Business Media

[3] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[4] Hunt, J and Cooke, D. 1996. Learning using an artificial immune system. Journal of Network and Computer Applications: Special Issue on Intelligent Systems : Design and Application. 19 189-212.

[5] Bakshi, A., & Dujodwala, Y. B. (2010, February). Securing cloud from ddos attacks using intrusion detection system in virtual machine. In 2010 Second International Conference on Communication Software and Networks (pp. 260-264). IEEE.

[6] Nikolai, J., & Wang, Y. (2014, February). Hypervisor-based cloud intrusion detection system. In 2014 International Conference on Computing, Networking and Communications (ICNC) (pp. 989-993). IEEE.

[7] Dasgupta, D (1998). An overview of artificial immune systems. Artificial Immune Systems and Their Applications. 3-19. Springer-Verlag

[8] Mafraq, J. Proposed anticipating learning classifier system for cloud intrusion detection (ALCS-CID). Probe, 4107, 0-83.

[9] Kholidy, H. A., Erradi, A., Abdelwahed, S., & Azab, A. (2014, August). A finite state hidden markov model for predicting multistage attacks in cloud systems. In 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing (pp. 14-19). IEEE.

[10] Gupta, M., Gao, J., Aggarwal, C., & Han, J. (2014). Outlier detection for temporal data. Synthesis Lectures on Data Mining and Knowledge Discovery, 5(1), 1-129.

[11] Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., & Khayam, S. A. (2013). A taxonomy of botnet behavior, detection, and defense. IEEE communications surveys & tutorials, 16(2), 898-924.

[12] Lee, Dong-Wook and Sim, Kwee-Bo. 1997. Artificial immune network based co-operative control in collective autonomous mobile robots. 58-63 Proceedings of IEEE International Workshop on Robot and Human Communication. Sendai, Japan. IEEE.

[13] Hu, W., Gao, J., Wang, Y., Wu, O., & Maybank, S. (2013). Online adaboost-based parameterized methods for dynamic distributed network intrusion detection. IEEE Transactions on Cybernetics, 44(1), 66-82.

[14] Butun, I., Morgera, S. D., & Sankar, R. (2013). A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16(1), 266-282.

[15] Kaur, R., & Singh, M. (2014). A survey on zero-day polymorphic worm detection techniques. IEEE Communications Surveys & Tutorials, 16(3), 1520-1549.

[16] Belouch, M., El Hadaj, S., & Idhammad, M. (2018). Performance evaluation of intrusion detection based on machine learning using Apache Spark. Procedia Computer Science, 127, 1-6.

[17] Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016, February). Long short term memory recurrent neural network classifier for intrusion detection. In 2016 International Conference on Platform Technology and Service (PlatCon) (pp. 1-5). IEEE.

[18] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. Ieee Access, 5, 21954-21961.

[19] Mohd, N., Annapurna, S., & Bhadauria, H. S. (2014). Taxonomy on Security Attacks on Self Configurable Networks. World Applied Sciences Journal, 31(3), 390-398.

ANNEXURE –A

TABLE. A. LIST OF ABBREVIATIONS

S.No.	**Abbreviations**	**Description**
1.	IDS	Intrusion Detection System
2.	LAN	Local Area Networks
3.	AIS	Artificial Immune System
4.	IDPS	Intrusion Detection and Prevention Systems
5.	NBA	Network Behavior Analysis
6.	DMZ	Demilitarized Zone
7.	KMP	Knuth-Morris-Pratt Substring Algorithm
8.	Ipv4	Internet Protocol Version 4
9.	Ipv6	Internet Protocol Version 6
10.	IDA	Interruption Detection Arrangements