www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6751-6755

Research Work on Network Intrusion Detection Using Artificial Immune System

Vijeta[1], Mr. Vivek Sharma[2]

[1]M.tech scholar (CSE),JMIT Radaur
Kurukshetra University,
Vijeta1191@gmail.com

[2]Head of the Computer Science and Engineering Deptt,
JMIT Radaur, Kurukshetra University
Vivek@jmit.ac.in

Abstract: ***An artificial immune system (AIS) is a computer software system that mimics some parts of the behavior of the human immune system to protect computer networks from viruses and similar cyber attacks. Artificial immune system is a computer software system that mimics some parts of the behavior of the human immune system to protect computer networks from viruses and similar cyber attacks. The essential idea is that the human immune system, which is a complex system consisting of lymphocytes. This work provides AIS based intelligence to provide security measures in intrusion detection system.***

Keywords: Intrusion detection Systems, Computer Security, Evolutionary algorithms, Artificial Immune System

1. INTRODUCTION

The natural immune system is a broad area of search in today's era of research because of its information processing capabilities. HIS has ability to perform several complex computations in a parallel and distributed fashion[1]. For example; the nervous system, immune system has feature of learning new information, recall this previously learned information and performs pattern recognition tasks in a de-centralized fashion and also uses a distributed detection and response mechanism in order to respond to foreign invaders. There arises a question for developers; as we know that HIS[2]can detect and defend against harmful and previously unseen invaders, so can a similar system be built for our computers? Perhaps, those systems would then have the same beneficial properties as the HIS such as error tolerance, adaptation and self monitoring.

This feature gives us an idea that the security in computing may be considered as analogous to the immunity in natural systems. In computing, because of a malfunction of components or intrusive activities both internal and externals threats and dangers may arise. This problem of protecting computer systems from harmful viruses can be view as a problem of distinguishing self (legitimate users, uncorrupted data, etc.) from dangerous other (unauthorized users, viruses, and other malicious agents), and to predict the future behavior of system or system's processes based on the present and past states i.e. if the actual state of the system differs from the predicted state, an anomaly alarm is raised. Therefore, A challenge is arise to build an anomaly detection system that can capture multi-variable correlations, and is capable of dealing with the large amount of data generated in a computer network environment. However, to determine the nature of current and future threats in conjunction with in larger IT systems requires the development of automate and adaptive defensive tools.

A great and promising solution is using biologically inspired computing, and mainly artificial immune systems (AIS)[3][4],Because one can see an analogy between the HIS and IDS. The HIS has both innate and adaptive components to its mechanisms, like for example; an innate response is inflammation – the attraction of lymphocytes to the site of an injury and their automatic consumption of dead cells. An adaptive response is a response learned during the lifetime of an organism, such as the production of specific antibodies from carefully maintained populations of B cells. The innate part of the HIS is a kin to the misuse detector class of IDS. Similarities can also be drawn between the adaptive immune system and anomaly based IDS. Both the innate HIS and misuse detectors have prior knowledge of attackers and detect them based on this knowledge. Similarly, both the adaptive immune system and anomaly detectors generate new detectors to find previously unknown attackers [4].

The objective of this research paper is to create a simulating environment for evaluation of Naïve string search algorithm

based upon bio inspired algorithm. Test developed Network Intrusion Detection System to protect a machine or collection of machines from unauthorized intruders or differentiate the self and non-self strings. We take IPv4 addresses as string for testing our algorithm. Such a research is now important, as a sufficiently large body of research has been amassed to take stock and consider what further avenues should be explored in the future. [5]

2. EVOLUTIONARY ALGORITHMS

An Evolutionary algorithm is a subset of evolutionary computation, a generic population-based meta-heuristic optimization algorithm [6]. An EA uses mechanisms inspired by biological evolution, such as reproduction, mutation, recombination, and selection. Candidate solutions to the optimization problem play the role of individuals in a population, and the fitness function determines the quality of the solutions. Evolution of the population then takes place after the repeated application of the above operators. Artificial evolution (AE) describes a process involving individual evolutionary algorithms; EAs are individual components that participate in an AE.

Evolutionary algorithms often perform well approximating solutions to all types of problems because they ideally do not make any assumption about the underlying fitness landscape; this generality is shown by successes in fields as diverse as engineering, art, biology, economics, marketing, genetics, operations research, robotics, social sciences, physics, politics and chemistry. Evolutionary algorithms (EAs) and other bio-inspired algorithms have been widely used to solve complex search problems, including optimization problems. The taxonomy shown below includes Evolutionary computation (EC) is a paradigm in the artificial intelligence realm that aims at benefiting from collective phenomena in adaptive populations of problem solvers utilizing the iterative progress comprising growth ,development, reproduction, selection, and survival as seen in a population .

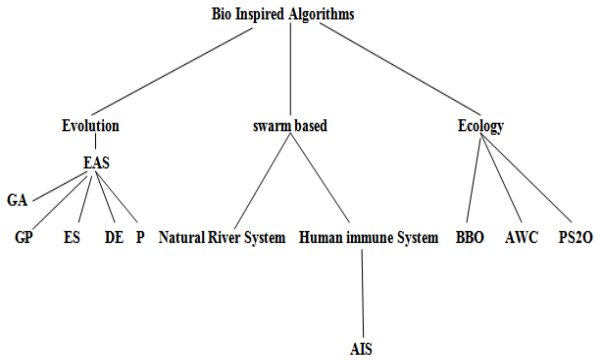

Fig-1.Taxonomy and nomenclature of various bio inspired optimization algorithms grouped by the area of inspiration [7].

EAs are the most well known, classical and established algorithms among nature inspired algorithms, which is based on the biological evolution in nature that is being responsible for the design of all living beings on earth, and for the strategies they use to interact with each other.

A family of successful EAs comprises genetic algorithm (GA), genetic programming (GP), Differential Evolution, evolutionary strategy (ES) and most recent Paddy Field Algorithm.

I. ***GENETIC ALGORITHM***-GAs are among the most successful class of algorithms under EAs which are inspired by the evolutionary ideas of natural selection. The three principal genetic operators in GA involve selection, crossover, and mutation.

II. ***GENETIC PROGRAMMING***- GP is an extension to Genetic algorithms differs from the latter in terms of representation of the solution. The steps in Genetic programming involve:

- Generate an initial population of computer programs comprising the functions and terminals.
- Execute each program in the population and assign it a fitness value according to how well it solves the problem.
- Create a new population of computer programs.
  a. Copy the best existing programs
  b. Create new computer programs by mutation.
  c. Create new computer programs by crossover.

III. ***EVOLUTION STRATEGIES***-Evolution Strategies is a global optimization algorithm inspired by the theory of adaptation and evolution by means of natural selection.

IV. ***DIFFERENTIAL EVOLUTION***-DE is similar to GAs since populations of individuals are used to search for an optimal solution. The main difference between Gas and DE is that, in GAs, mutation is the result of small perturbations to the genes of an individual while in DE mutation is the result of arithmetic combinations of individuals. At the beginning of the evolution process, the mutation operator of DE favors exploration. As evolution progresses, the mutation operator favors exploitation. Hence, DE automatically adapts the mutation increments to the best value based on the stage of the evolutionary process.

V. ***PADDY FIELD ALGORITHM***- PFA constitutes following five basic steps.

- ***Sowing:*** The algorithm operates by originally scattering seeds (initial population p0) at random in an uneven field.

- ***Selection:*** Here the finest plants are selected based on a threshold method so as to selectively weed out unfavorable solutions and controls the population.

- ***Seeding:*** In this stage every plant develops a number of seeds proportional to its health. The seeds that drop into the main favorable places (most fertile soil, best drainage, soil moisture etc.) tend to produce to be the best plants (taller) and produce more number of seeds.

- ***Pollination:*** For seed propagation pollination is a chief factor either via animals or through wind. High population density would boost the chance of pollination for pollen carried by the wind

- ***Dispersion*****:** In sort to prevent getting stuck in local minima, the seeds of each plant are discreted .Depending on the status of the land it resolve grow into new plants and persist the cycle.

VI. ***SWARM INTELLIGENCE***-It is an expansion of EC. While EAs are supported on genetic adaptation of organisms SI is based on shared social behavior of organisms.SI can be described by judging five fundamental principles.

- ***Proximity Principle:*** the population should be capable to carry out simple space and time computations.
- ***Quality Principle:*** the population should be able to react to quality factors in the environment.
- ***Diverse Response Principle****:* the population should not give its activity along excessively narrow channels.
- ***Adaptability Principle****:* the population should be able to alter its behavior mode when it is worth the computational price.
- ***Stability Principle****:* the population should not modify its mode of behavior every time the environment changes.

Swarm intelligence includes a lot of algorithm Particle Swarm Optimization: In PSO, the term particles refers to population members which are mass-less and volume-less (or with an arbitrarily small mass or volume) and are question to velocities and accelerations towards a better mode of behavior.

VII. ***ARTIFICIAL IMMUNE ALGORITHM***- An increasing amount of work is being carried out attempting to understand and extract the key mechanisms through which the HIS is able to achieve its detection and protection capabilities. A numeral of AIS has been built for a wide range of applications including document classification, network- and host-based, and fraud detection intrusion detection.These AIS have met with some success and in many cases have rivaled or bettered existing statistical and machine learning techniques. Two significant mechanisms dominate AIS research: [8]

1. Network-based models
2. Negative selection models

Artificial Immune algorithm is found on colonal selection principle [9] and is a population based algorithm .AIS is stimulated by the human immune system which is a highly evolved, parallel and distributed adaptive system that exhibits the following strengths: immune recognition, feature extraction, immune memory, diversity, reinforcement learning, and robustness. The steps in AIS are as follows:

- ***Initialization*** of antibodies (potential solutions to the problem). Antigens symbolize the value of the objective function f(x) to be optimized.

- ***Cloning***, where the affinity or fitness of every antibody is determined. Based on this fitness the antibodies are replicated; that is the most excellent will be cloned the most.

- ***Hyper mutation*****:** The clones are next subjected to a hyper mutation process in which the clones are mutated in inverse proportion to their affinity; the finest antibody‘s clones are mutated lesser and worst antibody‘s clones are mutated mainly.

Immune Algorithms belong to the Artificial Immune Systems field of study concerned with computational methods inspired by the process and mechanisms of the biological immune system. A simplified description of the immune system is an organ system intended to protect the host organism from the threats posed to it from pathogens and toxic substances. Pathogens encompass a range of micro-organisms such as bacteria, viruses, parasites and pollen. The traditional perspective regarding the role of the immune system is divided into two primary tasks: the detection and elimination of pathogen. This behavior is typically referred to as the differentiation of self (molecules and cells that belong to the host organisms) from potentially harmful non-self. These interrelated immunological sub-systems are comprised of many types of cells and molecules produced by specialized organs and processes to address the self-nonself problem at the lowest level using chemical bonding, where the surfaces of cells and molecules interact with the surfaces of pathogen.

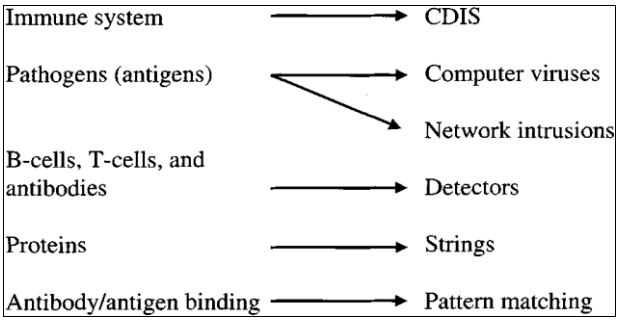

Fig.2-Biological to computational domain top-level mapping

3. PROPOSED WORK

In designing any swarm based systems which is in particularly targeted towards Network Intrusion Detection, we must to certain principles that

- The immune system should be diverse, which greatly improves robustness, on both a population and individual level, for example, different people are vulnerable to different microbes; in case of networks the system should be able to detect large IP swarm in case of Denial of Service Attacks.
- It should be distributed, consisting of many components that interact locally to provide global protection, so there is no central control and hence no single point of failure.
- It should be error tolerant in that a few mistakes in classification and response are not catastrophic.
- It should be dynamic in nature, i.e. individual components are continually created, destroyed, and are circulated throughout the body, in case of Network the system should be able to detect any type of Addressed for example IPv4 or IPv6 regardless.

4. CONCLUSION

The immune system is considered to provide both defence and maintenance of the body. There are many reasons why the immune system has been seen as a source of inspiration for the design of novel algorithms and systems. This thesis was about using Naïve String Search algorithm for use in Artificial immune system, the general Naïve string searching algorithm finds all occurrences of one given string within another. It has running time complexity is proportional to the sum of the lengths of the strings and the modified algorithm can also be extended to deal with some more general pattern matching problems.

We developed Algorithms that were bio inspired and provided simulations for Network intrusion detection scenarios. The Algorithm used the adaptive Naïve string search algorithm as Pattern Matching algorithm to mimic the behavior of a human Lymphocyte. The algorithm proved to be successful and the results were satisfying. In future we will Improve Lymphocyte performance for IPv4 and especially IPv6 Networks.

5. ACKNOWLEDGMENT

I would like to extend my sincere thanks and greetings to Vivek Sharma, Head of the Department of Computer science & Engineering, JMIT RADAUR, Haryana, India for his kind help, moral support and guidance in preparing this article.

No of Lyphocytes	IPv4 Detection Time(AVG)
1	0.513
2	0.68
3	0.7
4	0.85
5	0.88
…	…
15	1.43
16	1.41
17	1.52
18	1.41
20	1.41

Table 1: IPv4 Detection Time v/s No of Lymphocytes

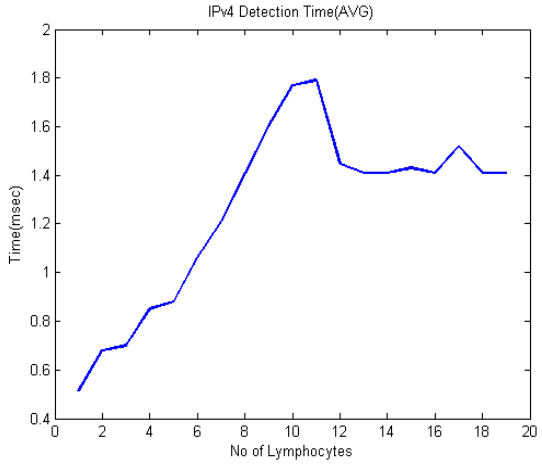

Fig 3: IPv4 Detection Time v/s No of Lymphocytes

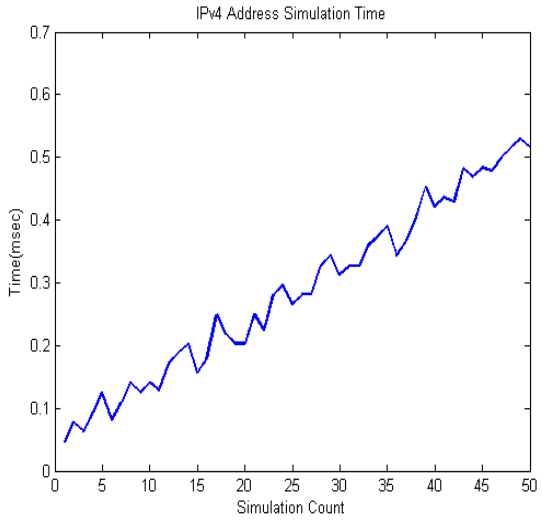

Fig 4: Graph showing IPv4 Simulation time

REFERENCES

[1] Kari, Lila, and Grzegorz Rozenberg. "The many facets of natural computing." Communications of the ACM 51.10 (2008): 72-83.

[2] Sakaguchi, Shimon, Makoto Miyara, Cristina M. Costantino , and David A. Hafler. "FOXP3+ regulatory T cells in the human immune system." Nature Reviews Immunology 10, no. 7 (2010): 490-500.

[3] Luger, George F. Artificial intelligence: Structures and strategies for complex problem solving. Pearson education, 2005.

[4] Dasgupta, Dipankar, and Fernando Nino. Immunological computation: theory and applications. CRC Press, 2008.

[5] Basu, M. "Artificial immune system for dynamic economic dispatch." International Journal of Electrical Power & Energy Systems 33, no. 1 (2011): 131-136.

[6] Greensmith, Julie, Uwe Aickelin, and Jamie Twycross. "Detecting danger: applying a novel immunological concept to intrusion detection systems." arXiv preprint arXiv:1002.0696 (2010).

[7] Binitha, S., and S. Siva Sathya. "A survey of bio inspired optimization algorithms." International Journal of Soft Computing and Engineering 2, no. 2 (2012): 137-151.

[8] Grefenstette, John J., David E. Moriarty, and Alan C. Schultz. "Evolutionary algorithms for reinforcement learning." arXiv preprint arXiv:1106.0221 (2011).

[9] Brownlee, Jason. "Clonal selection algorithms." Complex Intelligent Systems Laboratory, Swinburne University of Technology, Australia (2007).

[10] Laurentys, C. A., G. Ronacher, Reinaldo M. Palhares, and Walmir M. Caminhas. "Design of an artificial immune system for fault detection: A negative selection approach." Expert Systems with Applications 37, no. 7 (2010): 5507-5513.

[11] Anil Somayaji, Steven Hofmeyr, & Stephanie Forrest "Principles of a Computer Immune System " .1997 New Security Paradigms Workshop Langdale, Cumbria UK Copyright ACM 1998 0-89791-986–6.

[12] Steven A. Hofmeyr and Stephanie Forrest,"Immunity by Design: An Artificial Immune System".

[13] Jungwon Kim and Peter J. Bentley,"An Evaluation of Negative Selection in an Artificial Immune System for Network Intrusion Detection".Department of Computer Science,University College London.

[14] Mark Handley and Vern Paxson,"Network Intrusion Detection: Evasion,Traffic Normalization, and End-to-End Protocol Semantics".AT&T Center for Internet Research at ICSI (ACIRI) International Computer Science Institute Berkeley, CA 94704 USA.

[15] Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, and Gary B. Lamont,"An Artificial Immune System Architecture for Computer Security Applications".IEEE Transactions On Evolutionary Computation, Vol. 6, No. 3, June 2002

[16] J. Timmis P. Andrews N. Owens E. Clark,"An interdisciplinary perspective on artificial immune systems".Springer-Verlag, DOI 10.1007/s12065-007-0004-2,2008

Authors Profile

Vijeta received her B.tech degree in Computer Science & Engineering from Yamuna Institute of Engineering & Technology(YIET) in 2012 and Now pursuing her M.tech from Seth Jai Parkash Mukand Lal institute of engineering and technology(JMIT). Her area of interests includes Network Security, Intrusion Detection and Prevention, Web Security.