International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

A Review on Network Intrusion Detection using Artificial Immune System (AIS)

[1.] Vijeta, [2.] Mr. Vivek Sharma
[1.] M.Tech Scholar(C.S.E), JMIT Radaur,Haryana,India
[2.] Head of the Deptt(C.S.E Deptt), JMIT Radaur, Haryana,India

***Abstract*— Computer systems are evolving to be more and more exposed to attack this is the reason computer security has become a vital concern for network. Intrusions cause disaster inside LANs. Intrusion Detection Systems (IDS) are used to monitoring information about them and reporting them to security administrators. An important and natural application domain for adaptive systems swarm based is that of computer security. A computer security system should protect a machine or collection of machines from unauthorized intruders. The system should also be able prevent against foreign code, which is similar in functionality to the immune system protecting the self from invasion by microbes. An 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. Survey in this field present the need of a Novice substring search algorithm based upon bio inspired algorithms and Test to developed Network Intrusion detection System to protect a machine or collection of machines from unauthorized intruders.**

Keywords*— Intrusion Detection System-IDS, Artificial Immnue System-AIS,Human Immune System

I. 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. 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 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 and 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 that 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 automated And adaptive defensive tools. A great and promising solution is using AIS.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. The objective of this review paper is to provide an overview of IDS for AIS researchers to identify suitable intrusion detection research problems, and to provide information for IDS researchers about current AIS solutions. Such a review 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.[1][2].

A. INTRUSION DETECTION SYSTEM

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of probable incidents, which are violations or threats of violation of computer security strategies, adequate used policies, or usual security practices. Intrusive events to computer networks are expanding because of the more use of the internet and local area networks.[3][4][5].

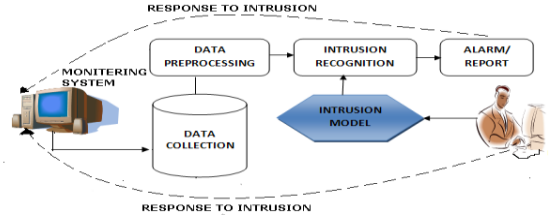

Fig-1. General process of intrusion Detection

→METHODOLOGIES OF IDS

Intrusion detection system uses many methodologies to detect incidents. [3]

A. Signature based Detection-A signature is a pattern of string that corresponds to a known threat. This is process of comparing signatures of occurring events to identify an intrusion. It is a very effective process for detecting known threats but largely ineffective in detecting previously unknown threats.

B. Anomaly based Detection-Anomaly based detection will search for something rare or unusual. They analyses system event to find patterns of activity that appears to be abnormal. Anomaly based detection is a process of comparing behavior of running events against observed normal events to identify significant deviations.

→TECHNIQUES OF IDS

IDS use several techniques to protect itself from attackers explain below.

A.Host-based Intrusion detection system-Host-based IDS or HIDS are installed as agents on a host computer. HIDS can look into system and application log files to detect any intruder activity. Some HIDS systems are reactive i.e. they inform host only when something wrong is happened. On the other side some HIDS are proactive in nature i.e. they can sniff the network traffic coming to a particular host on which the HIDS is installed and alert host in real time.

B.Network-based Intrusion detection system-NIDS is an intrusion detection systems at network level that capture data packets traveling on the network media (Cables, wireless) and perform a matching of them with database of known intruder signatures, whether a packet is matched with an intruder signature, an alert message is generated or the packet is logged to a file or database.

→TYPES OF NETWORK ATTACKS

A. Denial of Service (DoS)-A DoS attack is a type of attack in which the attacker makes a memory/computing resources too busy to serve legitimate networking requests and denying users access.For example ping of death, back, mail bomb etc.

B. Remote to User Attacks (R2L)-IN R2L attack a user sends packets to a machine over the internet, to which s/he is not allow to access .S/he try to expose the machines vulnerabilities and exploit privileges which a local user have on the computer.[5]

C. User to Root Attacks (U2R)-In U2R attack a user starts access on the system as a normal user account and after some time s/he try to abuse vulnerabilities of the system in order to gain super user privileges.

D. Probing-Probing is a kind of attack in which the intruder scans a network in order to determine vulnerabilities or topology information of the system and save them in their system for later exploitation of the machine or networking.

→ WHERE IDS SHOULD BE PLACED IN NETWORK TOPOLOGY?

Depending upon your network topology, you can place intrusion detection systems at one or more places. It also depends upon what kind of intrusion activities you want to detect: internal, external or both. For example, if you want to detect only external intrusion activities, and you have only one router connecting to the Internet, then the best place for an intrusion detection system is with the router or a firewall and if you have multiple paths to the Internet, you can place one IDS box at every entry point. However if you want to detect internal threats as well, you can place a box in every network segment. Fig-b shows locations where you can place an intrusion detection system.[6][11]

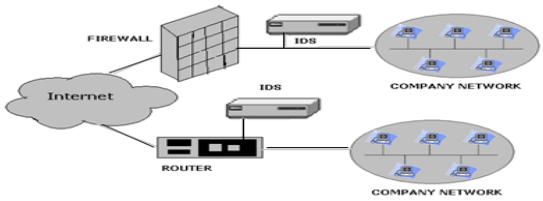

Fig-2. Locations for an intrusion detection system

B. HUMAN IMMUNE SYSTEM

Human immune system is a network of cells, tissues, and organs all of these work together to protect the body against attacks by "foreign" invaders. The secret of its Success is an elaborate and dynamic communications network. Millions of cells, organized into sets and subsets, gather like clouds of bees swarming around a hive and pass information back and forth in response to an infection. After detection, immune cells receive the alarm and they become active and begin to produce powerful chemicals. The key of healthy immune system is its remarkable ability to distinguish between the body's own cells, recognized as "self," and foreign cells, or "non-self."

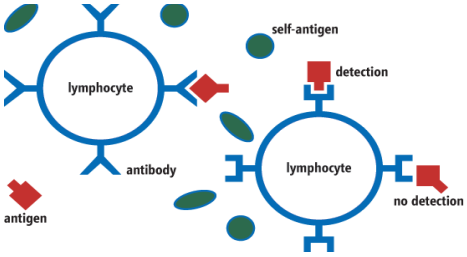

Fig-3. Elements of a Simplified Immune System

The organs of the immune system are placed in whole body of human being; they are called lymphoid organs because they are home to lymphocytes, small white blood cells that are the key players in the immune system. Bone marrow, soft tissue in the hollow center of bones, is the ultimate source of all blood cells, including lymphocytes. Lymphocytes known as T lymphocytes or T cells ("T" stands for "thymus"). B lymphocytes, also known as B cells, become activated and mature into plasma cells, which make and release antibodies. Lymphocytes can travel throughout the body using the blood vessels. The cells can also travel through a system of lymphatic vessels that closely parallels the body's veins and arteries.

C. ARTIFICIAL IMMUNE SYSTEM (AIS)

There exists many computational technique that inspired by biology, for example; evolutionary algorithms genetic algorithm and AIS or immunological computation. Biological immune system is a subject of research interest because of its information processing feature. The immune system may be used to solve the computer-virus problem has been suggested by Dasgupta and S. Forrest. [14]

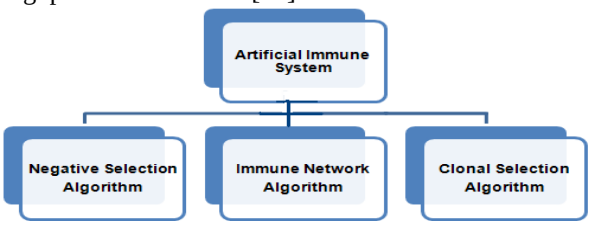

Fig-4. Different Mechanisms of AIS

Several AIS models have been built for a wide range of applications including document classification, fraud detection, and network & host-based intrusion detection.

These AIS system have met with success and in several cases proved better than existing statistical and machine learning techniques. Important mechanisms dominate AIS research:

A. Immune Network Models-The immune Network theory proposed the hypothesis that the immune system maintains an idiotypic network of interconnected B cells for antigen recognition. These cells both stimulate and suppress each other in certain ways that lead to the stabilization of the network. Two B cells are connected if the affinities they share exceed a certain threshold [7][8][9].

B.Clonal Selection Principle- This Principle describes the basic features of an immune response to an antigenic stimulus. It establishes the idea that only those cells that recognize the antigen proliferate, thus being selected against those that do not.

C.Negative Selection Algorithms-The purposes of this algorithm is to recognize all cells within the body and categorize those cells as self or non-self. It deals with the immune system's ability to detect unknown antigens while not reacting to the self cells.

D. IDS RESEARCH PROBLEMS FOR AIS

We summarize the following requirements of IDS that must be fulfill by AIS:[1][2]

Properties of IDS	Related Problems
Robustness	It should have multiple detection points with low operational failure rates which are resilient to attack
Configurability	It should be able to configure itself easily to the local requirements of Host or network component.
Extendibility	It should be easy to extend the Scope of IDS monitoring by and for new hosts easily and simply regardless of operating systems
Scalability	It is necessary to achieve reliable scalability to gather and analyses the high-volume of audit data correctly from distributed hosts
Adaptability	It should adjust time in order to detect dynamically changing network intrusions
Efficiency	It should be simple & lightweight enough to impose a low overhead on the monitored host systems and network

Table-1.IDS Research Problems

E. AIS FEATURES FOR IDS

The piece of work by Somayaji et al. identifies immune features that are desirable for an effective IDS.[11][12]

A. Distributed-IDS support robustness, configurability, extendibility and scalability. It can also scale better, since the high volume of audit data is distributed amongst many local hosts and is analyzed by those hosts.

B.Self-Organized-Self-organizing IDS provides global analysis and adaptability. Without external management or maintenance, self-organizing IDS automatically detects intrusion signatures which are previously unknown and eliminates them.

C.Lightweight- Lightweight IDS supports efficiency and dynamic features. A lightweight IDS does not impose a large overhead on a system or place a heavy burden on CPU and I/O. It places minimal work on each component of the IDS.

D.Multi-Layered- Multi-layered IDS increases robustness. The failure of one layer defenses does not necessarily allow an entire system to be compromised. While a distributed IDS allocates intrusion detection processes across several hosts, a multi-layered IDS places different levels of sensors at one monitoring place.

E.Diverse-Diverse IDS provides robustness. A variety of different intrusion detection processes spread across hosts will slow an attack that has successfully compromised one or more hosts. This is because an understanding of the intrusion process at one site provides limited or no information on intrusion processes at other sites.

F.Disposable-Disposable intrusion system (IDS) increases robustness, extendibility and configurability. A disposable IDS does not depend on any single component. Any component can be easily and automatically replaced with other components.

II. RELATED WORK

AIS algorithm have been applied in various fields by researcher; among them, the clonal selection algorithm with negative selection developed for computer security in networks is especially motivated by the work performed by Forrest et al (1993) and Smith et al (1993). ***Forrest et al (1994; 1997)*** proposed a negative selection algorithm for anomaly detection problems. This algorithm differentiates 'self' and 'non-self' systems by building normal behavior patterns of a monitored system. This algorithm generates a number of patterns that are compared to each self pattern defined. If any randomly generated pattern matches a self pattern, this pattern is removed. Otherwise, it becomes a 'detector' pattern and monitors subsequent profiled patterns of the monitored system.

Anil Somayaji, Steven Hofmeyr (1997) works on computer security principles and suggests that natural immune systems provide a rich source of inspiration for computer security in the age of the Internet. Immune systems have many features that are desirable for the imperfect, uncontrolled, and open environments in which most computers currently exist. These include disreputability, diversity, disposability, adaptability, autonomy, dynamic coverage, anomaly detection, multiple layers and identity via behavior, no trusted components, and imperfect detection. These principles suggest a wide variety of architectures for a computer immune system Good passwords, appropriate access controls, and careful design are still needed for good security. They focused on the human immune system's adaptive responses.

Jungwon Kim, Peter J. Bentley et al. described that the use of artificial immune systems in intrusion detection is an appealing concept for two reasons. Firstly, the human immune system provides the human body with a high level of protection from invading pathogens, in a robust, self-organized and distributed manner. Secondly, current techniques used in computer security are not able to cope with the dynamic and increasingly complex nature of computer systems and their security. It is hoped that biologically inspired approaches in this area, including the use of immune-based systems will be able to meet this challenge. They summarized six immune features that are desirable in effective IDS: distributed, multi-layered, self-organized, lightweight, diverse and disposable.

Dipankar Dasgupta et al. (1995, 1998, 2002, and 2006) present a technique that inspired by the negative selection mechanism of the immune system that can detect foreign patterns in the complement (non-self) space. In particular, the novel pattern detectors (in the complement space) are evolved using a genetic search, which could differentiate varying degrees of abnormality in network traffic. The immune system has the property that foreign invaders (i.e., the non-self) are recognized easily with few false positives. This process proceeds in two stages: in the first stage, the non-self is identified as a novelty (novelty detection), and the immune system then preserves a long-term memory for this pattern. They investigated an immune-computing technique to evolve novel pattern detectors in the complement pattern space to identify any changes in the normal behavior of monitored behavior patterns. This technique (NC) is used to characterize and identify different intrusive activities by monitoring network traffic, and compared with another approach (PC).

Paul K. Harmer, Paul D. Williams (2002) described that with increased global connectivity, reliance on e-commerce, network services, and computer security has become a necessity. Organizations must protect their systems from intrusion and computer-virus attacks. Such protection must detect anomalous patterns by exploiting known signatures while monitoring normal computer program and network Usage for abnormalities. Today's network intrusion detection (ID) solutions can become overwhelmed by the burden of capturing and classifying new viral stains and intrusion patterns. To overcome this problem, a self-adaptive distributed agent-based defense immune system based on biological strategies is developed within a hierarchical layered architecture. A prototype interactive system is designed, implemented in Java and tested. The results validate the use of a distributed-agent biological-system approach toward the computer-security problems of virus elimination and ID. The level of effectiveness is tunable through the proper selection of the number of antibodies, antibody length and the detection threshold. These must be selected based on the contents of known self and with an understanding of their ramifications on negative selection time, scan time, and non-self space coverage. The use of the agent paradigm facilitates the construction of AIS because of the performance limitations of a monolithic implementation and the biological basis for the architecture can be viewed as a system of collaborating agents. The ability of these facets working together promises an enterprise- wide computer-security solution. At the heart of CDIS is the ability to proactively generate antibodies capable of detecting non-self data.

III. AIS APPLICATIONS AREA FOR IDS

Artificial Immune Systems is used in many applications such as anomaly detection, pattern recognition, data mining, computer security, adaptive control and fault detection. Among these two applications are considered as solution of real-world problems. [7][8][9].

A.Application in Computer Security-The role of the immune system can be considered same as that of computer security systems, Host-based IDS methods construct a database that catalogues the normal behavior during the system calls made. Dasgupta argue that this approach is not expensive computationally and can be easily used in real time. It also has the advantage of being platform and software independent. An alternative method is the network-based intrusion detection approach tackles the issue of protecting networks of computers rather than an individual computer. This is achieved in a similar way in monitoring network services, traffic and user behavior and attempts to detect misuse or intrusion by observing departures from normal behavior. Work in laid foundations for a possible architecture and the general requirements for an immunity-based intrusion detection system by using the metaphor of the innate immune system, which resides on the user's PC and applies virus-checking heuristics to .com and

.exe files. If an unknown virus is detected, then a sample is captured that contains information about the virus and is sent to a central processing system for further examination.[13]

B.Application in Fault Detection-The field of fault diagnosis needs to accurately predict or recover from faults occurring in plants, machines like refrigeration systems, communications like telephone systems and transportations like Aircrafts. In the field of fault diagnosis, there has also been some interest in creating distributed diagnostic systems. Initial work by H. Bersini proposed a parallel-distributed diagnostic algorithm. However, the authors likened their algorithm to that of an immune network, due to its distributed operation, and the systems emergent co-operative behavior between sensors. In an interesting work by T. Oda and T. White involving Aircraft Fault detection, experiments were performed with datasets collected through simulated failure conditions using NASA Ames C-17 flight simulator. Three sets of in-flight sensory information namely- body-saxes roll rate, pitch rate and yaw rate, were considered to detect five different simulated faults: one for Engine, two for the Tails and two for the Wings.A real-valued negative selection algorithm, called MILD, was utilized to detect a broad spectrum of known as well as unforeseen faults.Once the fault was detected and identified, a direct adaptive control system utilized the detection information to stabilize the aircraft by utilizing available resources. The MILD software tool implements an immunity-based technique for anomaly and fault detection where a small number of specialized detectors (as signatures of known failure conditions) and a set of generalized detectors for unknown (or possible) fault conditions are. Once the fault is detected and identified, an adaptive control system would use this detection information to stabilize the aircraft by utilizing available resources.[10]

IV. CONCLUSION

This review paper pressents the analogy between the HIS and IDS naturally that attracts computer scientists to research on immune system approaches to intrusion detection. Artificial immune system (AIS) is a broad area of research because of its powerful information processing capabilities, understanding the distributed nature of its memory, self-tolerance and decentralized control mechanisms from an informational perspective, and building computational models believed to better solve many science and engineering.As we know that the immune system has the property to recognised foreign intrusions (i.e., the non-self) with few false positives and by understanding the dynamics of the immune system, it is possible to implement a pattern recognition mechanism in the complement space where false positives and false negatives can be traded off.Through careful examination of literature presented in this paper, one can conclude that immunologically inspired IDS still have much room to grow and many areas to explore. Literature survey clearly illustrates that the history of research in this area has shown a clear focus on three major ideas:

- Methods inspired by the immune system that employ conventional algorithms, for example, IBM's virus detector.
- The negative selection paradigm as introduced by Forrest and Dasgupta.
- Approaches that exploit the Danger Theory.

Current work is now investigating the intrusion detection mechanism of the clonal selection stage by Kim and Bentley and Dasgupta.

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.

REFERENCES

[1] D. Dagupta and F. Gonz´alez "*An Immunity-Based Technique to Characterize Intrusions in Computer Networks*".IEEE Transactions on Evolutionary Computation, 6(3), pages 1081-1088 June 2002.

[2] Jungwon Kim,Peter J. Bentley, Uwe Aickelin, Julie Greensmith,GianniTedesco, JamieTwycross,*"Immune system Approaches to Intrusion Detection - A Review*". Natural Computing, Springer, in print, doi: 10.1007/s11047-006-9026-4, pp TBA.

[3] Lata, Indu Kashyap *"Study and Analysis of Network based Intrusion Detection System"*,International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013.

[4] Hassan, Mostaque Md Morshedur. *"Network Intrusion Detection System Using Genetic Algorithm And Fuzzy Logic."* International Journal Of Distributed And Parallel Systems (IJDPS) Vol.4, No.2, March 2013.

[5] Omprakash Chandrakar,Rekha Singh,*"Application of Genetic Algorithm in Intrusion Detection System",* ISSN 224-5774 (Paper) ISSN 2225-0492 Vol.4, No.1, 2014

[6] Rafeeq Ur Rehman,*"Intrusion Detection Systems with Snort"*.Prentice Hall PTR ISBN 0-13-140733-3,2003.

[7] Dipankar Dasgupta,"Advances in Artificial Immune Systems",IEEE Computational Intelligence Magazine November 2006.

[8] Binitha S, S Siva Sathya,"*A Survey of Bio inspired Optimization Algorithms*". International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307,Volume-2, Issue-2, May 2012.

[9] Anil Somayaji, Steven Hofmeyr, & Stephanie Forrest,*"Principles of a Computer Immune System".* Second New Security Paradigms Workshop, pages 75–82, 1997.20

[10] Steven A. Hofmeyr and Stephanie Forrest," *Immunity by Design: An Artificial Immune System*". Proceedings of GECCO, pages 1289-1296, 1999.

[11] 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. pp. 1244–1252, 2002

[12] 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.

[13] 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

[14] 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