A Novel Approach for Intrusion Detection to improve the detection rate using Artificial Immune system and Neural Network Technique

Akansha Parashar¹, Praneet Saurabh²

¹M.Tech, CSE, Technocrats Institute of Technology
Bhopal , M.P.
akansha.parashar1@gmail.com
²Professor, Technocrats Institute of Technology, Bhopal , M.P.
praneetsaurabh@gmail.com

Abstract

Research in the field of computer and network science demands for tools and methodology to test their security effectively. Intrusion Detection System is used to perform the same with a fact that an intruder’s behavior will be noticeably different from that of a legitimate user and would exploit security vulnerabilities. IDS have thousands of alerts per day; some are mistakenly triggered by benign events. This makes it extremely difficult to correctly identify alerts related to attack. 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. This research paper proposes a neural network approach to building a network-based IDS, which is inspired by an artificial immune system to find the unseen or unknown attack.

Key words: Intrusion detection system, Artificial Immune system, Neural Network,

1. Introduction

The primary function of a biological immune system is to protect the body from foreign molecules known as antigens. It has great pattern recognition capability that may be used to distinguish between foreign cells entering the body (non-self or antigen) and the body cells (self). Immune systems have many characteristics such as uniqueness, autonomous, recognition of foreigners, distributed detection, and noise tolerance (Castro and Zuben, 1999). Inspired by biological immune systems, Artificial Immune Systems have emerged during the last decade. They are incited by many researchers to design and build immune-based models for a variety of application domains. Artificial immune systems can be defined as a computational paradigm that is inspired by theoretical immunology, observed immune functions, principles and mechanisms (Castro and Timmis, 2003). This report investigates the different AIS computational paradigms and introduces different AIS models and techniques developed in the literature since the work of Dasgupta et al. (2003). The studied models are mainly based on the immune network theory, clonal selection principles and negative selection mechanisms. Computer security is used frequently, but the content of a computer is vulnerable to few risks unless the computer is connected to other computers on a network. As the use of computer networks, especially the Internet, has become pervasive, the concept of computer security has expanded to denote issues pertaining to the networked use of computers and their resources. The major technical areas of computer security are usually represented by the initials, confidentiality, integrity, and authentication or availability. Confidentiality means that information cannot be accessed by unauthorized parties. Confidentiality is also known as secrecy or privacy; breaches of confidentiality range from the embarrassing to the disastrous. Integrity means that information is protected against unauthorized changes that are not detectable to authorized users; many incidents of hacking compromise the integrity of databases and other resources. Authentication means that users are who they claim to be. Availability means that resources are accessible by authorized parties;
“denial of service” attacks, which are sometimes the topic of national news, are attacks against availability. Other important concerns of computer security professionals are access control and no repudiation. Security officers and show the kind of alerts first that the officer has previously been most interested. The field of artificial immune systems (AISs) is based on ideas and models that appear in biological immune systems. The AIS is a complex natural defense mechanism which, to some degree, is present in all living creatures. The AIS has the ability to learn about foreign substances (pathogens) in the body and to invoke the correct response to fight the infectious agents. In recent years, many artificial immune systems for network intrusion detection have been proposed. The main drawback of traditional methods is that they cannot detect unknown intrusion. Even if a new pattern of the attacks were discovered, this new pattern would have to be manually updated into system. It is also capable of identifying new attacks to some degree of resemblance to the learned ones, the neural networks are widely considered as an efficient approach to adaptively classify patterns.

Neural networks have been identified since the beginning as a very promising technique of addressing the intrusion detection problem the primary premise of neural networks that initially made it attractive was its generalization property, which makes it suitable to detect day-by-day attacks.

This research paper proposes a novel approach to building a network-based IDS, which is inspired by an artificial immune system to find the unseen or unknown attack Neural Network technique, allowing higher-level information, in the form of cluster membership, to be extracted the firewall and hit the protected system without a hitch. Besides, firewalls cannot stop insider attacks. On the contrary, anti-virus inspects executables (viruses or worms) or running process in memory of a protected system rather than network traffic to the system. Although anti-viruses monitor file integrity to protect against illegal data modification or so, they cannot stop malicious network traffic intended for network attacks, data-driven attacks, and so forth. Having all said that, typical functions of IDS include: (1) monitoring all or partial packets to detect hostile activities in real time (2) recording related event for later analysis (3) reporting network administrator to perform follow-ups.

2. Literature Survey

The ability of the IS to distinguish between self and non self is remarkable. This central mechanism of the IS is often modeled in AISs as various kinds of anomaly based detection. It should be noted that the IS is much more than a simple anomaly-based detection and response system; it can be viewed as a general pattern-learning system that is highly distributed and scalable. The pattern-learning abilities of the IS has been modeled and described by Timmis, Neal, and Hunt (2008) and Dasgupta, Cao, and Yang (2003) who successfully applied their AISs to recognition and classification tasks. They showed that their IS-inspired models were flexible, noise-tolerant and generalized their classification well. It has also been shown that it is possible to perform these tasks effectively with resource limited AISs (Timmis and Neal 2008). The behavior of the IS from an information processing perspective is described by Forrest and Hofmeyr (2001). In Seonin in 2002 tried to integrate a smart detection engine into a firewall and detecting unusual structures in data packets uses a classical feed-forward multi-layer perceptron network: a back propagation neural network and time delay neural network to program-based anomaly detection. Also Byoung-Doo in 2006 built IDS deals well various mutated attacks, as well as well-known attacks by using Time Delay Neural Network classifier that discriminates between normal and abnormal packet flows. It seems that the area where the notion of AIS has been most widespread is in the area of computer security. This idea has been explored in general by Somayaji, Hofmeyr, and Forrest (1998), Burgess (1998), Dasgupta (2007), Hofmeyr (2008) and Hofmeyr and Forrest (2009).

This work has focused both on computer security architectures as a whole and on specific areas of computer security. The areas in computer security where AISs have been used, at least experimentally, range from virus detection (Forrest et al. 2008), as a kind of host-based anomaly detection, and OS process monitoring (Forrest et al. 1996) to NID (Hofmeyr and Forrest 2009; Williams et al. 2008), as a kind of distributed network-based anomaly detection.

To overcome low detection rate and high false alarm problems in currently existing IDS, we propose a hierarchical off line Anomaly intrusion detection system using Distributed Time-Delay Artificial Neural Network to enhance the performance of intrusion detection for rare and complicated attacks. In this paper, we introduce anomaly intrusion detection system, this can detect network-based attacks using dynamic neural nets, and has facilities for training, testing, and tuning of dynamic nets for intrusion detection purpose.
3. Background of IDS and AIS

This section gives a brief introduction to two distinct fields of study - IDS and AIS, setting the background to and defining the terminology used in the sections that follow.

3.1 Intrusion Detection System

An Intrusion Detection System (IDS) constantly monitors actions in a certain environment and decides whether they are part of a possible hostile attack or a legitimate use of the environment. The environment may be a computer, several computers connected in a network or the network itself. The IDS analyzes various kinds of information about actions emanating from the environment and evaluates the probability that they are symptoms of intrusions. Such information includes, for example, configuration information about the current state of the system, audit information describing the events that occur in the system (e.g., event log in Windows XP), or network traffic. Several measures for evaluating IDS have been suggested (Debar et al. 1999; Richards 1999; Spafford and Zamboni 2000; Balasubramaniyan et al. 1998). These measures include accuracy, completeness, performance, efficiency, fault tolerance, timeliness, and adaptively. The more widely used measures are

The True Positive (TP) rate, that is, the percentage of intrusive actions (e.g., error related pages) detected by the system, False Positive (FP) rate which is the percentage of normal actions (e.g., pages viewed by normal users) the system incorrectly identifies as intrusive, and Accuracy which is the percentage of alarms found to represent abnormal behavior out of the total number of alarms. In the current research TP, FP and Accuracy measures were adopted to evaluate the performance of the new methodology. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat. We’ll cover each of these briefly.

3.1.1 Research Problems for AIS

The main objective of this review paper is to introduce suitable intrusion detection problems[9] to AIS researchers. Previously in [8] [10], Kim and Bentley have presented the requirements for an effective network-based IDS. These requirements can be applied not only to a network-based IDS, but to any type of IDS. These requirements are of particular interest because they could be fulfilled by mechanisms inspired by features of the human immune system.

Despite research conducted since the original publication of these requirements, no existing IDS model yet satisfies these requirements completely. We summaries these requirements here in order to analyze whether the existing AIS-based IDSs reviewed in this paper have provided some of these functions. The seven requirements reported in [12] are as follows:

- Robustness: it should have multiple detection points with low operational failure rates and which are resilient to attack
- Configurability: it should be able to configure itself easily to the local requirements of each host or each network component. Individual hosts in a network environment are heterogeneous.
- 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 analyze the high-volume of audit data correctly from distributed hosts.
- Adaptability: it should adjust over time in order to detect dynamically changing network intrusions.
- Global Analysis: in order to detect network intrusions, it should collectively monitor multiple events generated on various hosts to integrate sufficient evidence and to identify the correlation between multiple events.
- Efficiency: it should be simple and lightweight enough to impose a low overhead on the monitored host systems and network.

3.2 Artificial Immune Systems

The Human Immune System (HIS) protects the body against damage from an extremely large number of harmful bacteria, viruses, parasites and fungi, termed pathogens. It does this largely without prior knowledge of the structure of these pathogens. This property, along with the distributed, self-organized and lightweight nature of the mechanisms by which it achieves this protection [13], has in recent years made it the focus of increased interest within the computer science and intrusion detection communities. Seen from such a perspective, the HIS can be viewed as a form of anomaly detector with very low false positive and false negative rates.

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 number of AIS have been built for a wide range of applications including document classification, fraud detection, and...
network- and host-based intrusion detection [14]. These AIS have met with some success and in many cases have rivaled or bettered existing statistical and machine learning techniques. Two important mechanisms dominate AIS research: network-based models and negative selection models, although this distinction is somewhat artificial as many hybrid models also exist. The first of these mechanisms refers to systems which are largely based on Jerne’s idiotypic network theory[22][24] which recognizes that interactions occur between antibodies and antibodies as well as between antibodies and antigens. Negative selection models use the process of non-self matching selection, as seen with T-lymphocytes in the thymus as a method of generating a population of detectors. This latter approach (along with other newer algorithms)

has been by far the most popular when building IDS, as can be seen from the work.

3.2.2 AIS Technique

The common techniques are inspired by specific immunological theories that explain the function and behavior of the mammalian adaptive immune system.

• **Clonal Selection Algorithm:** A class of algorithms inspired by the clonal selection theory of acquired immunity that explains how B and T lymphocytes improve their response to antigens over time called affinity maturation.

These algorithms focus on the Darwinian attributes of the theory where selection is inspired by the affinity of antigen-antibody interactions, reproduction is inspired by cell division, and variation is inspired by somatic hyper mutation. Clonal selection algorithms are most commonly applied to optimization and pattern recognition domains, some of which resemble parallel hill climbing and the genetic algorithm without the recombination operator.

• **Negative Selection Algorithm:** Inspired by the positive and negative selection processes that occur during the maturation of T cells in the thymus called T cell tolerance. Negative selection refers to the identification and deletion (apoptosis) of self-reacting cells, that is T cells that may select for and attack self tissues. This class of algorithms is typically used for classification and pattern recognition problem domains where the problem space is modeled in the complement of available knowledge.

• **Immune Network Algorithms:** Algorithms that describes the regulation of the immune system by anti-idiotypic antibodies (antibodies that select for other antibodies). This class of algorithms focus on the network graph structures involved where antibodies (or antibody producing cells) represent the nodes and the training algorithm involves growing or pruning edges between the nodes based on affinity (similarity in the problems representation space). Immune network algorithms have been used in clustering, data visualization, control, and optimization domains, and share properties with artificial neural networks.

• **Dendritic Cell Algorithms:** The Dendritic Cell Algorithm (DCA) is an example of an immune inspired algorithm developed using a multi-scale approach. This algorithm is based on an abstract model of dendritic cells (DCs). The DCA is abstracted and implemented through a process of examining and modeling various aspects of DC function, from the molecular networks present within the cell to the behavior exhibited by a population of cells as a whole. Within the DCA information is granulated at different layers, achieved through multi-scale processing

3.2.3 AIS features for IDS

Although not the main objective, we also aim to provide information for IDS researchers about current AIS solutions in this article. In this section, we present AIS features that would be advantageous to novel IDS. Two previous papers [15] [16] have already covered this topic and here we summaries that work. Kim and Bentley presented three properties of IDSs that satisfy the seven requirements stated above [20] [21]. Another piece of work by Somayaji et al. [19] also identifies twelve immune features that are desirable for effective IDS.

We summaries these AIS features together after eliminating redundant properties:

• Distributed: a distributed IDS supports robustness, configurability, extendibility and scalability.

• It is robust since the failure of one local intrusion detection process does not cripple the overall IDS. It is also easy to configure a system since each intrusion detection process can be simply tailored for the local requirements of a specific host. The addition of new intrusion detection processes running on different operating systems does not require modification of existing processes and hence it is extensible. It can also scale better, since the high volume of audit data is distributed amongst many local hosts and is analyzed by those hosts.

• Self-Organized: A self-organizing [23] ID provides adaptability and global analysis. Without external
management or maintenance, a self-organizing
IDS automatically detects intrusion signatures

4. Proposed Approach

4.1 Neural Network :–

An Artificial Neural Network (ANN) is an
information-processing paradigm that is inspired by
the way biological nervous systems, such as the brain,
process information. The key element of this paradigm
is the novel structure of the information processing
system [17][18]. It is composed of a large number of
highly interconnected processing elements (neurons)
working in unison to solve specific problems. An ANN
is configured for a specific application, such as pattern
recognition or data classification, through a learning
process. Neural networks, with their remarkable
ability to derive meaning from complicated or
imprecise data, can be used to extract patterns and
detect trends that are too complex to be noticed by
either humans or other computer techniques. Neural
Network has other advantage

1. Adaptive learning: An ability to learn how to do
tasks based on the data given for training or initial
experience.

2. Self-Organization: An ANN can create its own
organization or representation of the information
it receives during learning time.

3. Real Time Operation: ANN computations may
be carried out in parallel, and special hardware
devices are being designed and

4. Manufactured which take advantage of this
capability.

5. Fault Tolerance via Redundant Information
Coding: Partial destruction of a network leads to
the corresponding degradation of

4.2 Growing Neural Gas Algorithm

Growing Neural gas is an neural network, inspired
by the self-organizing map and introduced in 1991 by
Thomas Martinetz and Klaus Schulten. The neural
gas is a simple algorithm for finding optimal data
representations based on feature vectors. The
algorithm was coined “neural gas” because of the
dynamics of the feature vectors during the adaptation
process, which distribute themselves like a gas within
the data space. The GNG algorithm only has
parameters that are constant in time and since it is
incremental, there is no need to determine the number
of nodes a priori. The issue of when GNG should
stop is discussed shortly.

GNG Algorithm

INIT: Create two randomly positioned nodes; connect them with a zero age edge and set their
errors to 0.

1. Generate an input vector $\vec{x}$ conforming to some
distribution.[16]

2. Locate the two nodes $s$ and $t$ nearest to , that is,
the two nodes with reference vectors $w_s$ and $w_t$
such that $s$ ?is the smallest value and 2 $w_s$ $t$
is the second smallest, for all nodes $k$.[9]

3. The winner-node $s$ must update it’s local error
variable so we add the squared distance between
$s$ and , to errors

4. Move $s$ it’s topological neighbours i.e. all nodes
connected to $s$ by an edge towards by fractions
$e_w$ and $e_n$ of the distance.

5. Increment the age of all edges from node $s$ to its
topological neighbours

6. If $s$ and $t$ are connected by an edge, then set the
age of that edge to 0. If they are not connected
then create an edge between them.

7. If there are any edges with an age larger than
$amax$ then remove them. If, after this, there are
nodes with no edges then remove these nodes.

8. If the current iteration is an integer multiple of
$\beta$ and the maximum node count has not been
reached, then insert a new node. Insertion of a
new node $r$ is done as follows:

- Find the node $u$ with largest error.
- Among the neighbours of $u$, find the node $v$
with the largest error.
- Insert the new node $r$ between $u$ and $v$ as
follows:

9. Create edges between $u$ and $r$, and $v$ and $r$, and
then remove the edge between $u$ and $v$.

10. Decrease the error-variables of $u$ and $v$ and set
the error of node $r$. [23]

11. Decrease all error-variables of all nodes $j$ by a
factor

12. If the stopping criterion is not met then repeat.
The criterion might be for example the
performance on a test set is good enough, or a
maximum number of nodes has been reached,
etc.

4.3 Evaluation Measures

To evaluate the system performance the following
measures (based on Sequeira and Zaki 2002) were
used.
True Positive Rate (TP) (also known as Detection Rate or Completeness): the percentage of terrorist pages receiving a rating above the threshold in the experiments, terrorist pages will be obtained from the users simulating terrorists.

False Positive Rate (FP): the percentage of regular Internet access pages that the system incorrectly determined as related to terrorist activities, i.e., the percentage of non-terrorist pages receiving a rating above threshold and suspected falsely as terrorists.

Accuracy: percentage of alarms related to terrorist behavior out of the total number of alarms. Since no benchmark data on content based intrusion detection is currently available, the results are compared to the best numbers achieved with ADMIT which is a command level method using the Means clustering algorithm to detect intruders (Sequeira and Zaki 2002).

5. Conclusion

This paper has investigated the use of artificial immune system for network intrusion detection.

6. References


We present a Neural Network based technique, which can be used to reduce the false positive in intrusion detection and improve the detection rate in intrusion detection.

The review conducted in this paper focused on providing an overview of IDS for AIS to identify suitable intrusion detection research problems. Information was also provided for IDS about current AIS solutions.

Intrusion detection systems aim to identify attacks with a high detection rate and a low false positive. Classification and data mining based method for intrusion detection is often ineffective in dealing with dynamic changes in intrusion patterns and characteristics. Consequently, unsupervised learning methods have been given a closer look for network intrusion detection.

Artificial immune system and Neural Networks using both supervised and unsupervised learning have many advantages in analyzing network traffic and identify to find out the unseen or unknown attack.


