International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

INTRUSION DETECTION SYSTEMS USING ARTIFICIAL IMMUNE SYSTEMS BASED ON DANGER THEORY

Harisha. M ,
B.Tech. Information Technology,
R.M.D Engineering College,
Chennai,India.

Mohana Prriya .S,
B.Tech. Information Technology,
R.M.D Engineering College,
Chennai,India.

Sushmithaa .M ,
B.Tech. Information Technology,
R.M.D Engineering College,
Chennai,India.

Vigilson Prem M ,
Professor,
Information Technology,
R.M.D.Engineering College.
Chennai,India.

Abstract: Intrusion Detection Systems (IDS) plays a very important role in cybersecurity. In this paper, we will introduce what is Intrusion Detection Systems (IDS), its role in cybersecurity. We will discuss on the available techniques to improve Intrusion Detection Systems (IDS). The Artificial Immune Systems (AIS) is also introduced and the techniques available in them are also glanced through in this paper. We will also introduce Danger Theory (DT) and how to use it to improve Intrusion Detection Systems (IDS).

I. INTRODUCTION

Cyber security refers to information security as applied to computers and networks, which is an important problem in the world today. This field covers all the processes and mechanisms by which computer based equipment, information and services are protected from unintended or unauthorized access, change, or destruction. With the development of the networks, computer security is facing enormous challenges. To solve this problem, Intrusion Detection Systems (IDSs) have become an indispensable component for detecting abnormal behaviors before they cause widespread damage. A detailed introduction about the Intrusion Detection Systems (IDS) is given in section 1.

A. Intrusion Detection System

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. An Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

There is a wide spectrum of IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyses incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as

malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system (IPS).

The IDS monitors traffics, and reports its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system. Attackers are capable of exploiting vulnerabilities very quickly once they enter the network, rendering the IDS an inadequate deployment for prevention device. Intrusion Detection System (IDS) is a type of security management system for computers and networks. An IDS system gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). IDSs use vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analysing both user and system activities
- Analysing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

Typically, an ID system follows a two-step process. The first procedures are host-based and are considered the passive component, these include: inspection of the system's configuration files to detect inadvisable settings; inspection of the password files to detect inadvisable passwords; and

inspection of other system areas to detect policy violations. The second procedures are network-based and are considered the active component: mechanisms are set in place to react to known methods of attacks and to record system responses.

The Intrusion detection methods are as follows.

- Signature-based/Misuse
- Anomaly-based/Statistical

1) Signature-based

A signature based IDS also known as misuse IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. This issue in that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to the IDS. During that lag time your IDS would be unable to detect the new threat.

2) Anomaly-based

An anomaly based IDS also known as statistical IDS will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network, what sort of bandwidth is generally used, what ports and devices generally connect to each other and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

3) Passive IDS

A passive Intrusion Detection Systems (IDS) detects the suspicious or malicious traffic and sends an alert to the administrator or user. It is up to the administrator or user to take action to block the activity or to respond in some or the other way.

4) Reactive IDS

A reactive Intrusion Detection System (IDS) not only detects suspicious or malicious traffic and alerts the administrator, it also takes predefined proactive actions to respond to the threat.

In simple terms, an Intrusion Detection Systems (IDS) can be compared with the burglar alarm.

An Intrusion Detection System (IDS) complements the firewall security. The firewall protects an organization from malicious attacks from the internet and Intrusion Detection System (IDS) detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security. Therefore, an Intrusion Detection System (IDS) could be defined as a security system that monitors computer systems and network traffic and analyses that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks from inside the organization. The components of IDS are discussed in section F.

5) Network attacks

- Denial Of Service (DOS)
- Remote To User Attacks (R2L)
- User To Root Attacks (U2R)
- Probing

6) Components of intrusion detection systems

An Intrusion Detection System (IDS) comprises of management console and sensors. Management console is the management and reporting console. Sensors are agents that monitor hosts or networks on a real time basis. An Intrusion Detection System has a database of signature attacks. The attack signatures are patterns of different types of previously detected attacks.

If the sensors detect any malicious activity, it matches the malicious packet against the attack signature database. In case it finds a match, the sensor reports the malicious activity to the management console. The sensor can take different actions based on how they are configured. For example, the sensor can reset the TCP connection by sending a TCP FIN, modify the access control list on the gateway router or the firewall or send an email notification to the administrator for appropriate action.

The existing IDS systems have a number of drawbacks.

- **More maintenance-** Unfortunately, the IDS will not replace a firewall, virus scan, or any other security measure. So when we install it, it will require additional maintenance effort and will not remove much, if any, of the existing burden. IDS are famous for setting off false positives-sounding the alarm when nothing is wrong. Although we can tweak the settings to reduce the number of false positives, you'll never completely eliminate the need to respond to false positives.
- **False negatives-** IDS can also miss intrusions. Technologies are improving, but IDSs don't always catch everything.
- **Staff requirements-** Proper management of an Intrusion Detection System requires experienced staff. The less experienced your staff, the more time they'll spend responding to false positives. Therefore, you will be creating not only more work for the IT department to handle, but also more difficult work in some cases.
- **Data overload-** Another aspect which does not relate directly to misuse detection but is extremely important is how much data can an analyst effectively and efficiently analyse. Being said that the amount of data we need to look at seems to be growing rapidly. Depending on the ID tools employed by a company and its size there is the possibility for logs to reach millions of records per day.

In order to overcome the above disadvantages, we combine a few techniques with the Intrusion Detection Systems. The techniques used to solve those shortcomings are discussed further in section 2.

B. Artificial immune systems

Nature has inspired us in many ways. One such inspiration from nature is the Human Immunology (HI) which serves as the best solution for computer security. Artificial Immune Systems (AIS) was one such solution for computer security from Human Immunology. Artificial Immune Systems (AIS) is a diverse area that attempts to serve as a bridge between immunology and engineering and is developed through the application of mathematical and computational modelling techniques to immunology. AIS have become an area of computer science and engineering that uses immune system

metaphors for the creation of novel solutions to problems. AIS is now much wider and is not confined to the development of new algorithms. AIS is moving into an area of true interdisciplinary and one of genuine interactions between immunology, mathematics and engineering.

Artificial Immune System (AIS) is the evolving technology now-a-days. Artificial Immune Systems (AIS) are the adaptive systems inspired by the Human Immunology (HI) and observed immune functions, principles and models, which are applied to the computational problem solving methods. The Artificial Immune System's original intention is to abstract the structure and function of the human immune system to computer systems. It is applied in solving the computational problems in mathematics, engineering, and information technology. AIS belong to the broader field of Artificial Intelligence (AI). It is a sub-field of biologically inspired computing and natural computation.

C. Combining artificial immune systems with intrusion detection systems

In order to combine AIS with IDS, there are three steps to be followed. The first step is to represent the elements of the system and interaction of individuals in an immune-like form. The goal of this step is to represent the ID elements in an immunology way and quantify the interaction of these elements by affinity measures. The abnormal behavior in IDS is presented as the antigen (non-self) in AIS. In ID domain, affinity means the similarity between detectors and data. Different representations can adopt different affinity measures. The second step is to generate the initial repertoires (generation algorithm), and the third step is to optimize the algorithm (evolution mode). More immune algorithms can be selected for these two steps. This framework can be thought of as a design procedure for engineer AIS inspired IDS. Thus AIS could be combined with IDS for a better solution to solve the problem of computer security.

In this paper we are going to discuss on how to implement the Intrusion Detection Systems (IDS) using Artificial Immune Systems (AIS) using an effective approach called Danger Theory (DT). The works related to Intrusion Detection Systems (IDS) are discussed in section 2.

II. RELATED WORKS

Many algorithms were devised and proposed in order to improve the Intrusion Detection Systems (IDS) [1]. The following are few techniques which are in existence for improving the IDS [16].

- Data mining techniques
- Genetic algorithm
- Fuzzy logic algorithm

A. Data mining techniques

Data mining is the process of analysing data from different perspectives and summarizing it into useful information. It allows user to analyse data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically data mining is the process of finding correlations or patterns among many fields in large relational databases [7].

Normal and intrusive activities leave evidence in audit data. From the data-centric point of view, intrusion detection is a data analysis process. The following are the few data mining techniques applied in IDS [17].

- **Association rule**- Association rules are created by analysing data for frequent if/then patterns and using the criteria support and confidence to identify the most important relationships. Support is an indication of how frequently the items appear in the database. Confidence indicates the number of times the if/then statements have been found to be true.
- **Classification**- Classification is a data mining technique that assigns items in a collection to target categories or classes. The goal of classification is to accurately predict the target class for each case in the data. Classification models are tested by comparing the predicted values to known target values in a set of test data.
- **Clustering techniques**- Clustering is a process of partitioning a set of data into a set of meaningful sub-classes, called clusters. It helps users understand the natural grouping or structure in a data set. In cluster analysis, we first partition the set of data into groups based on data similarity and then assign the label to the groups. Cluster analysis serves as a tool to observe characteristics of each cluster.
- **Decision tree**- Decision tree builds classification or regression models in the form of a tree structure. It breaks down a dataset into smaller and smaller subsets while at the same time an associated decision tree is incrementally developed. The final result is a tree with decision nodes and leaf nodes. Decision trees can handle both categorical and numerical data.
- **K-nearest neighbour**- In pattern recognition, the k-nearest neighbour algorithm (K-NN) is a non-parametric method used for classification and regression. In both the cases, the input consists of the k closest training examples in the feature space. K-NN is a type of instance-based learning, where the function is only approximated locally and all computation is deferred until classification.
- **Support vector machine**- Support Vector Machines (SVM), also called as Support Vector Networks are the models with associated support learning algorithms that analyse data used for classification and regression algorithms. In addition to performing linear classification, SVM can efficiently perform a non-linear classification using kernel trick.
- **Bayesian method**- Bayesian classification is based on Bayes' theorem. Bayesian classifiers are the statistical classifiers. Bayesian classifiers can predict class membership probabilities such as the probability that a given tuple belongs to a particular class.

The IDS combined with the data mining techniques and algorithms detects the threats and gives immediate response to the user. It also finds the detection rate, false alarm rate, and confidence level of the IDS. Applying data mining techniques on network traffic data is a promising solution to

improve IDS. But then, it has a few limitations which affect the effectiveness of the IDS [18].

1) Disadvantages

- Data mining does not provide the accurate data when goes beyond limits.
- The amount of data and complexity is more and increasing in data mining.
- The data mining is quite computationally expensive.
- Sometimes analysing network traffic without all the data could lead to false conclusions.

B. Genetic algorithm

A genetic algorithm (GA) is a method for solving both constrained and unconstrained optimization problems based on a natural selection process that mimics biological evolution. The algorithm repeatedly modifies a population of individual solutions. At each step, the genetic algorithm randomly selects individuals from the current population and uses them as parents to produce the children for the next generation. Over successive generations, the population "evolves" toward an optimal solution [19].

The following are the few terminologies used in Genetic Algorithm (GA).

- **Population-** It is a subset of all the possible encoded solutions to the given problem.
- **Chromosomes-** A chromosome is one such solution to the given problem.
- **Gene-** A gene is one element position of a chromosome.
- **Allele-** It is the value a gene takes for a particular chromosome.
- **Genotype-** Genotype is the population in the computational space.
- **Phenotype-** Phenotype is the population in the actual real world solution space in which solutions are represented in a way they are represented in real world situations.
- **Decoding and Encoding-** Decoding is a process of transforming a solution from the genotype to the phenotype space. Encoding is a process of transforming from the phenotype to the genotype space.

The following are the most important operators used in genetic algorithm.

- **Crossover-** The crossover operator is analogous to reproduction and biological crossover. In this, more than one parent is selected and one or more off-springs are produced using the genetic material of the parents. Crossover is usually applied in a GA with a high probability.
- **Mutation-** Mutation may be defined as a small random tweak in the chromosome, to get a new solution. It is used to maintain and introduce diversity in the genetic population and is usually applied with a low probability. If the probability is very high, the GA gets reduced to a random search.
- **Survivor selection-** The survivor selection policy determines which individuals are to be kicked out and which are to be kept in next generation. It is crucial as it should ensure that the fitter individuals are not kicked out of the population, while at the same time diversity should be maintained in the population.

Applying genetic algorithm to IDS decreases the false alarm rate. IDS upload and updates new rule to the system. Implementation of GA is unique as it considers both temporal and spatial information during encoding the problem. New rules are generated at run time, so administrator has no need to keep track of all these rules [20].

GA is used for evolving new rules for IDS. Using these rules normal network traffic or audit data is differentiated from abnormal traffic/data.

1) Disadvantages

- The GA may not find the global optimum when the population has a lot of subjects.
- The GA cannot assure constant optimisation response times.
- The GA applications in real time are limited because of random solutions and convergence.

C. Fuzzy logic algorithm

Fuzzy Logic Systems (FLS) produce acceptable but definite output in response to incomplete, ambiguous, distorted, or inaccurate fuzzy input. Fuzzy logic (FL) is a method of reasoning that resembles human reasoning. The approach of FL imitates the way of decision making in humans that involves all intermediate possibilities such as digital values YES or NO [21].

The conventional logic block that a computer can understand takes precise input and produces a definite output as TRUE or FALSE, which is equivalent to human's YES or NO. A fuzzy logic system can be defined as the non-linear mapping of an input data set to a scalar output data.

It is observed that unlike computers, the human decision-making includes a range of possibilities between YES and NO, such as-

- CERTAINLY YES
- POSSIBLY YES
- CANNOT SAY
- POSSIBLY NO
- CERTAINLY NO

The fuzzy logic works on the levels of possibilities of input to achieve the definite output [6].

The following are the basic concepts involved in FLS.

- **Approximation ("granulation")-** A colour can be described precisely using RGB values, or it can be approximately described as "red", "blue", etc.
- **Degree ("graduation")-** Two different colours may both be described as "red", but one is considered to be redder than the other fuzzy logic attempts to reflect the human way of thinking

The fuzzy logic controller performs three main actions which are as follows.

- **Fuzzification-** It is the process of changing a real scalar value into a fuzzy value.
- **Fuzzy processing-** The fuzzy processing involves evaluation of the input information according to IF…THEN rules.
- **Defuzzification-** Defuzzification is the process of producing a quantifiable result in crisp logic, given fuzzy sets and corresponding membership degrees.

1) Disadvantages

- The FLS algorithm is not suitable for highly accurate problems.
- The fuzzy system design does not have a systematic approach.
- When the solution is not known, the problem could not be solved using fuzzy logic.
- Fuzzy logic systems are expensive and it requires extensive testing

D. Intrusion Detection Systems using Artificial Immune Systems

The following are the algorithmic techniques in Artificial Immune Systems (AIS) used for developing Intrusion Detection Systems (IDS) [22].

- Negative Selection Algorithm (NSA)
- Artificial Immune Network (aiNET)
- Dendritic Cell Algorithm (DCA)
- Clonal Selection Algorithm (CSA) [2]

1) Negative Selection Algorithm

The Negative Selection Algorithm (NSA) is used for various anomaly detectors. The NSA defines 'self' by building the normal behaviour patterns of a monitored system. The algorithm generates a number of random patterns that are compared to each self-pattern defined [9]. If any randomly generated pattern matches a self-pattern, this pattern fails to become a detector and it is removed. Otherwise, it becomes a 'detector' pattern and monitors subsequent patterns. NSA is simple and easy to implement. If detectors are well generated, then the detection process can come up with good results [3].

a) Disadvantages

The main disadvantage of Negative Selection Algorithm is that self-elements do not remain the same through the whole time, they may change often. Continuous learning of the changing self-elements is a basic need in NSA so that detectors adjust themselves through time to be compatible with the self-components representation. Communication between detectors is also important to update their rules from time to time with new information.

2) Artificial Immune Network

The Artificial Immune Network (aiNET) can be used both for anomaly detection for detecting novel attacks and misuse detection for detecting known attacks and even variation from these attacks. The immune network provides a predictive capability to the detection of instances of misuse detection would identify the probability that a particular are event, or series of events. The immune network gains experience to improve the ability to determine where these events are likely to occur in the attack process [8]. This information could then be used to generate a series of events that should occur, is in fact an intrusion attempt. By tracking the subsequent occurrence of these events the system would be capable of improving the analysis of the events and possibly conducting defensive measures before the attack is successful.

Anomaly Detection is the model of normal behaviour of the system and they look for derivations from the normal behaviour as potential intrusions. To define a normal activity of the system in general is a very difficult task. For this purpose one can use neural networks the ability to learn the system with examples or trained with learning and their capability of abstraction. The learning ability shows that it is not necessary to define the normal behaviour of the system explicitly. Generalization allows the anomaly system to recognize when an attack has been muted slightly. The neural network should be able to recognize a variant of an attack that might be missed by misuse system. Also generalization may allow the anomaly system to recognize conditions that are typical of an attack in general.

a) Disadvantages

The main disadvantage in using neural networks is the training requirements of the neural network. Because the ability of the artificial neural network to identify indications of an intrusion is completely dependent on the accurate training of the system, the training data and the training methods are used critical.

3) Dendritic Cell Algorithm

The Dendritic Cells act as messengers between the innate and the adaptive immune systems. There are three main types of dendritic cells: 'immature' that collect parts of the antigen and the signals, 'semi-mature' that are immature cells that internally decide that the local signals represent safe and present the antigen to T-cells resulting in tolerance, and 'mature' cells that internally decide that the local signals represent danger and present the antigen to T-cells resulting in a reactive response [23].

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 [10]. Within the DCA information is granulated at different layers, achieved through multi-scale processing. The Dendritic Cell Algorithm improves the correlation factor, minimizing false positive and false negative alarm generation and increases the efficiency and accuracy of the IDS system.

a) Disadvantages

The main disadvantage of DCA is that it could not be applied to data where there is the potential for delayed antigen as performance may be impaired.

4) Clonal Selection Algorithm

In the Clonal Selection Algorithm (CSA), the selection is inspired by the affinity of antigen-antibody interactions, reproduction is inspired by cell division, and variation is inspired by somatic hyper mutation. The goal of the CSA is a pool of antibodies which represents a solution to the computational problems. In this algorithm, the antibody represents an element of a solution or a single solution to the problem, and the antigen represents an element or evaluation of the problem space [24].

The CSA is best suited for optimization and pattern recognition problems. It is a colony search mechanism in nature, which enables detectors to clone their parents

according to a mutation mechanism with high rates. This strategy evolves the immune systems so that they can deal with antigens that it has encountered in the past. From this, clonal selection could be combined with other methods to solve ID problems [5]. The clonal selection could be adopted as one component of the AIS for NID. Altogether, the CLONALG algorithm provides high detection rate (DR) and low false alarm rate (FA).

a) Disadvantages

The main disadvantage of CSA is premature convergence. The term premature convergence means that a population for an optimization problem converged too early, resulting in being suboptimal. In this context, the parental solution is not able to generate off-springs that are superior to their parents.

Although the above mentioned algorithms provide reasonable solutions, they do not completely meet the requirements of the Intrusion Detection Systems (IDS), since they have a number of disadvantages in their implementation [4]. The shortcomings of the above discussed related works could be overcome by the Danger Theory which is discussed in section 3 [25].

III. PROPOSED WORK

In order to overcome the disadvantages of previously mentioned algorithms which are used in Intrusion Detection Systems (IDS), the Danger Theory (DT) is introduced in this section.

A. The Danger Theory

The Danger Theory (DT) was originally inspired by the Human Immune System (HIS). It states that the immune system does not distinguish between self and non-self, but discriminates between dangerous and safe by recognition of pathogens or alarm signals from injured or stressed cells and tissues.

The danger theory suggests that the immune system reacts to threats based on the correlation of various danger signals, providing a method for grounding the immune responses by linking it directly to the attacker.

B. The Biology involved in Danger Theory

According to Danger Theory (DT) the most important thing for stimulating immune responses are normal tissues. When tissue cells are distressed because of injury, infection and so on, they start to secrete or express the "danger signals" on their surface. In case, if the stressed cell dies by immunologic non-silent cell death such as necrosis or proptosis (as opposed to apoptosis, controlled cell death), the "Danger signals" are thrown out to extracellular space. This model also dictates that despite their potential immunogenicity tumours do not induce significance immune responses which could destroy malignant cells. According to the danger theory, the immune surveillance system fails to detect tumour antigens because transformed cells do not send any danger signals which could activate dendritic cells and initiate an immune response. "Danger signals" are normal intracellular molecules which are not in extracellular space among physiological conditions. The danger theory has evolved over the years. "Danger signals" include DNA, RNA, Heat Shock Proteins (HSPs), hyaluronic acid, serum amyloid A protein, ATP, uric acid and also cytokinesis like interferon alpha, interleukin-1 beta, CD40L and so on.

The Danger model has brought a new sight of adaptive and innate immunity. In the past the innate immunity was suggested as a minor part of immune system and opposite to the adaptive part was thought to be the most important and most effective one. According to danger theory there is no adaptive immunity without the innate immunity.

In further sections, the algorithm which could implement Danger Theory in IDS is discussed.

C. Danger Theory Algorithm

Danger Theory (DT) algorithm is an algorithm which emulates the defense mechanism of the Human Immune System (HIS) when presented with a danger in a computational context. The Human Immune System (HIS) based on danger theory has developed a complex defense mechanism against entities which are harmful to the human body. This system is divided into two sub-systems that provide different types of defense, the innate immune system that is activated by generic harmful entities to the human body, and the adaptive immune system which is activated by specific antigens. The main inspiration for its concept is the capacity of the Human Immune System (HIS) which responds to the human body flexibly and efficiently. If Danger Theory (DT) is implemented, we can take care of 'non-self but harmless' and of 'self but harmful' invaders into our system.

Applying ideas from the Danger Theory (DT) can help in building a better Artificial Immune system (AIS) by providing a different way of grounding and removing the necessity to map self or non-self. To achieve this self and non-self-discrimination will be useful. This is because non-self no longer causes an immune response. It is the danger signals that trigger a reaction. The following theory was proposed and drawn based on the fig1.

Danger theory (DT) is not about the way by which Artificial Immune System that represents data. Instead, it provides ideas about which data the Artificial Immune systems should represent and deal with. They should focus on dangers and send the signals.

The danger theory supports the need for discrimination. Instead of responding to the foreign elements that enters the body, the immune system reacts to the danger. There is no need to react to every foreign element. When the cells die an unnatural death, the distress signals are sent out to measure the danger created by the damaged cells. A distressed cell sends out an alarm signal, the antigens in the neighborhood are captured by Antigen Presenting Cells (APC) such as macrophage; they travel to the local lymph node and present the antigens to lymphocytes. In this scenario, the danger signal establishes a danger zone around itself. Once the danger signal has been transmitted, the immune system can react to those antigens, which are 'near' the danger signal emitter. 'Near' means something that makes sense for connections and their IP addresses but not for computer executables. In essence, the physical 'near' that the Danger

Theory (DT) requires for the immune system is a proxy measure for causality.

The B cell undergoes the clonal expansion process and also produces the antibodies that match the antigens within the danger zone and gets stimulated. The antibodies that do not match with the antigens or that is far away from the antigens do not get stimulated. Hence, we can substitute it with more appropriate causality measures such as similar execution starts times, concurrent runtimes or access of the same resources.

Consequently, those antibodies or detectors that match (first signal) those antigens with the radius, defined by a measure such as the second signal, will proliferate. Having thereby identified the dangerous components, further confirmation could then be sought by sending it to a special part of the system simulating another attack. This would have the further advantage of not having to send all detectors to confirm danger. Using these ideas Danger Theory (DT) has provided a better grounding of danger labels in comparison to self or non-self, at the same time it relies less on human competence.

The nature of the danger signal is unclear the signal might be positive or negative. The signal will not be an abstract representation of danger; it is rather grounded. This theory is explained in the above diagram.

However, Danger Theory provides an effective way to approach the problem of Intrusion Detection Systems (IDS). The Danger Theory is capable of providing effective novel attack detection with minimal administrative effort.

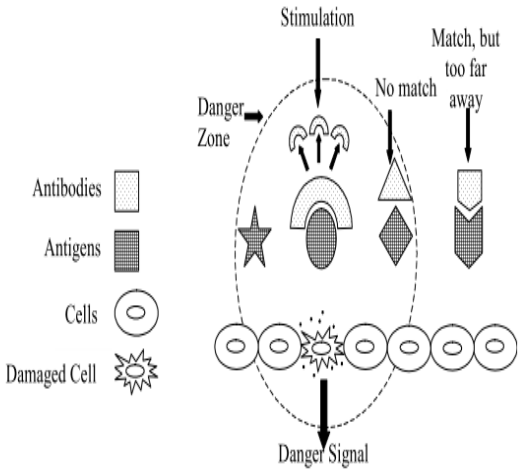

Fig. 1. Danger Model Diagram.

D. *The Danger Theory algorithm*

The following algorithm is proposed in order to support the Intrusion Detection Systems (IDS) using Danger Theory (DT) based on the above mentioned theory:

1) The algorithm for danger theory

begin
for all antigens
if an unnatural death occurs to a do
send a signal to the detector;
capture the antigens using antigen presenting cells;
if the danger signal is emitted do
react to the antigens near the danger signal emitter;
match the antibodies with the radius of the antigens;
identify the dangerous components;
react to the danger; do not react to the foreign element;
establish a danger zone around the danger signal;
undergo clonal expansion;
produce the antibodies;
if antibodies match with the antigens in the danger zone do
stimulate them;
else
do not stimulate the antibodies;
end for
end

IV. CONCLUSION

This approach might have a few disadvantages when the IDS are executed exactly as suggested by this theory. Despite the limitations, several suggestions are proposed in order to modify these aspects to support the IDS. These modifications provide the necessary platform to work for the development of DT inspired IDS. This type of detector has the potential to overcome such limitations associated with misuse and anomaly detectors. Especially, the development of a robust signal selection scheme and an appropriate correlation algorithm would realize these potential detectors.

REFERENCES

[1] E. Kesavalu Reddy, Member IAENG, Neural Networks for Intrusion Detection and its Applications, In Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013, July 3-5, 2013, London, U.K.

[2] R.Sridevi, Dr.Rajan Chattamvelli, Dr.E.Kannan, R.Sridevi et al, / (IJCSIT), Analysis of Human Immune System Inspired Intrusion Detection Sysrem, International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011, 2335-2339.

[3] Inadyuti Dutt, Samarjeet Borah, Indrakanta Maitra, Intrusion Detection Sytem using Artificial Immune System, International Journal of Computer Applications (0975-8887), Volume 144-No.12, June 2016.

[4] Uwe Aickelin, Steve Cayzer, The Danger Theory and its Application to Artificial Immune Systems, In Proceedings of the 1st Internet Conference on Artificial Immune Systems (ICARIS-2002), pp 141-148, Canterbury, UK, 2002.

[5] Pavitra Chauhan, Nikita Singh, Nidhi Chandra, A Review on Intrusion Detection System based on Artificial Immune System, Intenational Journal of Computer Applications (0975-8887), Volume 63-No.20, February 2013.

[6] R. Ravinder Reddy, Dr. Y Ramadevi, Dr. K. V. N Sunitha, Fuzzy Logic and Genetic Based Intrusion Detection System, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, August 2015.

[7] Abhaya, Kaushal Kumar, Ranjeeta Jha, Sumalya Afroz, Data Mining Techniques for Intrusion Detection: A review, International Journal of Advanced Research in Computer and Communication Engineering, Vol 3, Issue 6, June 2014.
[8] Sonam Lowry, Manish Singhal, IDS using Immune Network Clustering Via J48, International Journal in Multidisciplinary and Academic Research, Vol.2, No.4, July-August (ISSN 2278-5973).
[9] Salim Chikhi, Chikh Ramdane, A new Negative Selection Algorithm for Adaptive Network Intrusion Detection System, International Journal of Information Security and Privacy, Volume 8 Issue 4, October 2014.
[10] Kalpana Kumari, Prof. Anurag Jain, Prof. Aakriti Jain, Intrusion Detection Technique based on Dendritic Cell Algorithm and Dempster Belief Theory, IOSR Journal of Computer Engineering (IOSRJCE), Volume 1, issue 5 (May-June 2012).
[11] https://en.wikipedia.org/wiki/Intrusion_detection_system
[12] https://www.slideshare.net/amiable_indian/data-mining-and-intrusion-detection
[13] https://www.sans.org/security-resources/idfaq/data-mining-in-intrusion-detection/2/14
[14] https://www.mathworks.com/discovery/genetic-algorithm.html
[15] http://scialert.net/fulltext/?doi=itj.2013.2167.2173
[16] https://en.wikipedia.org/wiki/Fuzzy_logic
[17] https://en.wikipedia.org/wiki/Artificial_immune_system
[18] https://en.wikipedia.org/wiki/Dendritic_cell
[19] https://en.wikipedia.org/wiki/Clonal_selection
[20] https://en.wikipedia.org/wiki/Danger_model