IOSR Journal of Computer Engineering (IOSRJCE)
ISSN : 2278-0661 Volume 1, Issue 5 (May-June 2012), PP 38-43
www.iosrjournals.org

Intrusion Detection Technique based on Dendritic Cell Algorithm and Dempster Belief Theory

[1]Kalpana Kumari [2]Prof. Anurag Jain [3]Prof. Swati Dongre [4]Prof. Aakriti jain
[1]*M.Tech. Scholar Deptt.of CSE RITS,Bhopal*
[2, 3,4Asst]*. Prof. Deptt.of CSE RITS, Bhopal*
[4Asst]*. Prof. Deptt.of CSE SIRT ,Bhopal*

Abstract: *Today traditional intrusion detection systems are unable to detect intrusion attacks. Huge number of false alarm generated by the system results in financial loss of an organization. The unique features of artificial immune system encourage and motivate the researchers to employ this technique in variety of applications and especially in intrusion detection systems. Recently Artificial immune system (AIS) has been applied for anomaly based intrusion detection in computer networks. Artificial immune system is a new technique which is applied for solving various problems in the field of information security. In this paper we presents a intrusion detection system based on one of the algorithm of artificial immune system called the Dendritic Cell Algorithm (DCA) and Dempster–Belief Theory (DBT) in order to minimise the rate of the generation of intrusion detection system , false positive rate and improve correlation factor in the designed intrusion detection system. With the help of Dempster–Belief theory we calculate the degree of uncertainty and with the help of event gathering calculate the entropy, which help us to determine the intrusion in the given system. Data having higher entropy is regarded as the "intruder" and generate the alarm. Thus with the help of this dual detection technique we can not only minimize the false positive and false negative rate but also improved the correlation technique and decrease the intrusion rate in the system.*

Keywords- *Artificial Immune System, intrusion detection system, human immune system, danger theory, negative selection algorithm, DCA, Dempster–Belief theory.*

I. Introduction

Intrusion Detection Systems are one of the important building blocks of a secure, reliable network and are used widely along with the other security programs and concepts. There are several methods used to implement intrusion detection such as statistical analysis expert systems and state transition approaches etc. and these several approaches are based on the immune system were proposed in recent years. The main goal of Intrusion Detection System is to detect unauthorized use, misuse and abuse of computer systems by both systems insiders and external intruders. It can be a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

Artificial Immune System is a new bio-inspired model, which is applied for solving various problems in the field of information security, genetic algorithms, neural networks, evolutionary algorithms and swarm intelligence. AIS is defined as "Adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models"[1]. In addition to AIS pioneers, over the past ten years there has been a lot of works on application of AIS in computer security and utilizing it in intrusion system.

AIS is inspired from human immune system (HIS) which is a system of structures in human body that recognize the foreign pathogens and cells from human body cells and protect the body against those disease [2]. The human immune system has some features such as self-organized system, automated system, distributed system etc., which are now IDS starve for. So artificial immune system theory for detecting intrusion becomes a new approach in security research.

The objective of this paper is to propose a novel intrusion detection system to identify all intrusion correctly and minimized the false alarm generation. The Dendritic Cell Algorithm (DCA) and Dempster–Belief theory (DBT) along with the concept of entropy is used to designed the system in order to improve precise value of alarm generation which increase the performance of the system. The dendritic cell algorithm solve the problem of correlation by correlating the signal and this work also be done by the antigen system and Dempster–Belief theory is a mathematical theory of evidence able to detect previously unknown and rapidly evolving harmful attacks.

This paper is divided into V sections. Section II describes about the intrusion detection system and its various techniques. Section III deals with related work associated with the intrusion detection system based on artificial immune system. Section IV describes our new proposed method in the field of network security for intrusion

detection system based on artificial immune system using the concept of Dendritic Cell Algorithm and Dampeser – Belief theory. Finally we draw some brief conclusion in section V.

II. About the intrusion detection system and its various techniques

(a) Intrusion detection system

An intrusion is the set of actions that an illegal user manages to gain unauthorized access, or a legal user exceeds or misuses his privileges. It also includes the set of actions that attempt to cause entire systems and Networks crashed, running efficiency decreased, or service denied. An intrusion detection system (IDS) is the tool that attempts to detect intrusions and collect the evidences of intrusion for data restoration and event treatment [3].

Intrusion detection systems (IDS) focus on exploiting attacks, or attempted attacks, on networks and systems, in order to take effective measures based on the system security policies, if abnormal patterns or unauthorized access is being suspected .However, there are two potential mistakes by IDS, namely, false positive error (FPE) and false negative error (FNR). For FPE and FNE a pattern is mistakenly determined as abnormal normal respectively [3].

There are basically two types of intrusion detection system:

- host-based intrusion detection system
- And network-based intrusion detection systems.

Host based intrusion detection system uses system and audit logs as a source while network uses network traffic its source. Each approach has its respective strength and weakness. Some of the attacks can be detected only by host or only by network based intrusion detection system.

(b) Classification of various techniques Used in intrusion detection system

There are several different kinds of techniques used to design Intrusion detection system. These include statistical anomaly techniques, fuzzy logic techniques, rule-based anomaly techniques, rule-based penetration identification, state transition techniques, neural network based, data mining techniques etc.

In recent there are various techniques introduces for the implementation of intrusion detection system. In our system we statistical techniques for the detection of intrusion [9]. The statistical anomaly detection is also called Bayesian method. There are basically two types of detection techniquesin statistical approach.

- misuse detection and
- anomaly detection

In order to handle unknown attacks, the anomaly detection method is used. Their aim is to improve the detection and false alarm rates generated by the system.Misuse detection identify intrusions by matching its broad applicability to different fields. Some of the observed data with pre-defined descriptions of intrusive behaviour. Therefore, well-known intrusions can be detected efficiently with a very low false alarm rate. For this reason, the approach is widely adopted in the majority of commercial systems. Misuse detection will fail easily when facing unknown intrusions. One way to address this problem is to regularly update the knowledge base, either manually which is time consuming and laborious, or automatically with the help of supervised learning algorithms [9]. Unfortunately, datasets for this purpose are usually expensive to prepare, as they require labelling of each instance in the dataset as normal or a type of intrusion. Another way to solve this problem is to follow the anomaly detection model.

Anomaly detection has the capability of detecting new types of intrusions, and only requires normal data when building profiles [3]. However, its major difficulty lies in discovering boundaries between normal and abnormal behaviour, due to the deficiency of abnormal samples in the training phase. Another difficulty is to adapt to constantly changing normal behaviour, especially for dynamic anomaly detection. Figure1 explain the types of Anomaly detection method used in the detection system. There are two types of anomaly detection:

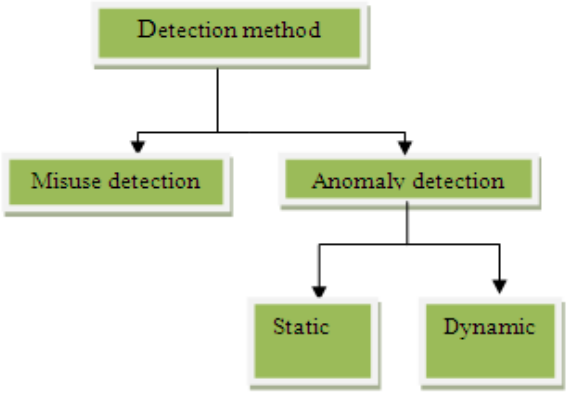

Figure1. Types of Anomaly detection

- The first is static anomaly detection, which assumes that the behaviour of monitored targets never changes, such as system call sequences of an Apache service.
- The second type is dynamic anomaly detection. It extracts patterns from behavioural habits of end users, or usage history of networks/hosts. Sometimes these patterns are called profiles.

Clearly, anomaly detection has the capability of detecting new types of intrusions, and only requires normal data when building profiles. However, its major difficulty lies in discovering boundaries between normal and abnormal behaviour, due to the deficiency of abnormal samples in the training phase. Another difficulty is to adapt to constantly changing normal behaviour, especially for dynamic anomaly detection [3].

III. Related work

In recent years use of Artificial immune system (AIS) has been favoured by the researcher to build Intrusion Detection Systems based on it. Although this idea has not been completely applied to the current IDS, but a lot of effort has been made to develop this idea. The primitive theoretical study on artificial immunology has been conducted by Farmer in 1986 [4]. They put forward a new link between biological and computing science [1]. Forrest et al in 1994 purposed most effective idea in utilization of immunity in computer security for self and non-self discrimination. Uwe Aickelin [8] firstly introduced the theory to solve the recognition problem in the existing AISs.

Matzinger [7] in 2002 applied the Danger theory as alternative approach for self surrounding high false positive, poor adaptation and short self-monitored .Danger Theory states that the immune system will only respond when damage is indicated and is actively suppressed otherwise. Danger Theory is becoming an efficient way to solve problems such as classifications, and anomaly detections. Forrest firstly introduced immune principle into computer security.

They developed a negative selection algorithm (NSA) based on the principles of self/non- self discrimination in the human immune system [5]. This algorithm defines 'self' as normal behaviour patterns of a monitored system. It generates a number of random patterns. If any randomly generated pattern matches a self pattern, it fails to become a detector and will be removed. Otherwise, it becomes a 'detector' and is used to monitor subsequently access patterns. This whole process can be explain in figure 2.This algorithm operates on binary string, and adopts R-Contiguous Matching Function (RCMF) to determine a match degree between antibody and antigen[8].

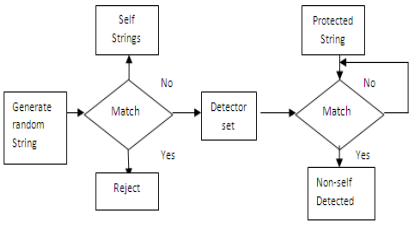

Figure2. Flowchart for the Generation of Detectors

For half a century, some fairly successful IDSs have been implemented, but were tarnished by issues surrounding high false positive, poor adaptation and short self-monitored.

IV. Our proposed Methodology

As one of the solutions to intrusion detection problems, Artificial Immune Systems (AIS) have shown their advantages. 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-organised and distributed manner.
- Secondly, traditional 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. In recent years the area of Artificial Immune System (AIS) has drawn attention of many significant application areas include optimization researchers due to problem , computer security , design of intrusion detection , fault detection , fault tolerance , pattern recognition, distributed learning, sensor network, Job-shop scheduling, design of recommendation system etc. The proposed architecture contains various modules each defined with a specific purpose and connected together to identify the exact intruder in the given system.

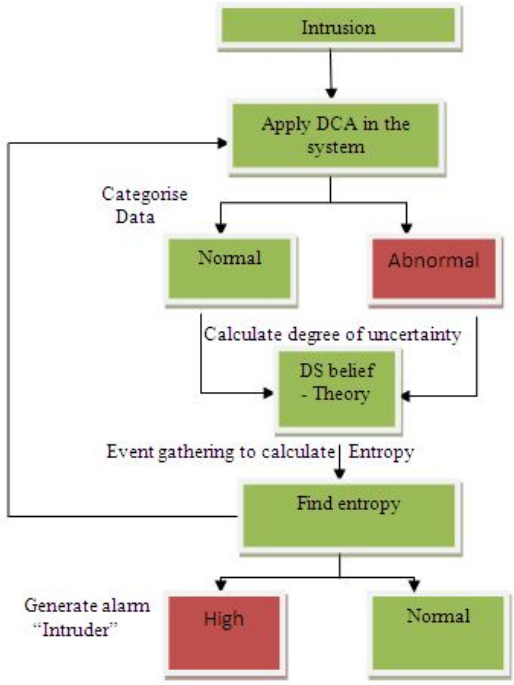

Figure3.Architecture of proposed intrusion detection system

Figure 3 shows the flow chart for the proposed new methodology for intrusion detection that is based on one of the algorithm of Artificial immune system called The Dendritic Cell Algorithm (DCA) and Dempster–Belief Theory (DBT) .The dendritic cell algorithm help us to solve the problem of correlation and Dempster–Belief Theory resolve the problem of unknown and rapidly evolving harmful attacks.

Integrating the "**Dendritic Cell Algorithm",** and **Dempster-Belief Theory** we proposes **"Intrusion detection technique based on Dendritic Cell Algorithm and Dempster Belief Theory".**

The main objectives of the resultant algorithm for various anomaly detection are:

- To improve the correlation factor,
- To minimized the false +ve and false –ve alarm generation and,
- To increase the rate of detection of intrusion

(a) Artificial immune system

Artificial Immune Systems in the literature can be define as "Artificial immune systems (AIS) are adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving". The AIS suggest a multilayered protection structure for protecting the computer networks against the unauthorized attacks [4].

The first generation of artificial immune system algorithms including negative selection and clonal selection do not produce the same high quality performance as the human immune system. These algorithms, negative selection in particular, are prone to problems with scaling and the generation of excessive false alarms when used to solve problems such as network based intrusion detection. The resulting algorithms are believed to encapsulate the desirable properties of immune systems including robustness, error tolerance, and self-organisation [4].

One such "second generation" AIS is the Dendritic Cell Algorithm (DCA) , inspired by the function of the dendritic cells (DCs) of the innate immune system. It incorporates the principles of a key novel theory in immunology, termed the "danger theory". This theory suggests that DCs are responsible for the initial detection of invading microorganisms, in addition to the induction of various immune responses against such invaders. An abstract model of natural DC behaviour is used as the foundation of the developed algorithm.

(b) Dendritic Cell Algorithm

The Dendritic Cell Algorithm (DCA) is not a classification algorithm, but shares properties with certain filtering techniques. It provides information representing how anomalous a group of antigen is, not simply if a data item is anomalous or not. This is achieved through the generation of an anomaly coefficient value, termed the MCAV – mature context antigen value [10]. The labelling of antigen data with a mature context antigen value coefficient is performed through correlating a time-series of input signals with a group of antigen. The signals used are pre- normalised and pre-categorised data sources, which reflect the behaviour of the system being

monitored. The signal categorisation represents the degree of normal and abnormal data and categorised into mainly three categories:

- **PAMP**: A measure that increases in value as the observation of anomalous behaviour. It is a confident indicator of anomaly, which usually presented as signatures of the events that can definitely cause damage to the system.
- **Danger**: A measure indicates a potential abnormality. The value increases as the confidence of the monitored system being in abnormal status increases accordingly.
- **Safe**: A measure that increases value in conjunction with observed normal behaviour. This is a confident indicator of normal, predictable or steady-state system behaviour.

Biological signal	Function	Abstract signal/signal used in DCA	Function
pamp	Indicator of microbial presence	Pamp signal	Signature of likely anomaly
Necrotic signal	indicator of tissue damage	Danger signal	High level indicate potential anomaly
Apoptotic signal	indicator of healthy tissue	Safe signal	High level indicate normal data

Table 1.Signal in Human immune system and in DCA

According to the results, the DCA has shown not only good performance in terms of detection rate, but also the ability to reduce the rate of false alarms in comparison to other systems, including Self Organising Maps [10].
The goal of the DCA is to incorporate such a relationship to identify antigens that are responsible for the anomalies reflected by signals. Table1. Represent the correlation between biological signal used in the Human immune system and the signal used in the DCA.
With the help of **Dendritic Cell Algorithm** we categorised data, whether the data is normal or affected with anomaly or we can say, abnormal.

(c) Occurrence event possibility

We have set up possible event .Each of which we assumed , occurs some numbers of times. Thus if there are n distinct possible event X1,X2,.....Xn, and the event occurred frequency N1,N2,.....Nn. Now measure the probability of event is

$$P(xi) = \frac{ni}{\sum_{j=1}^{N} nj}$$

Now measured entropy, represented by H(x) is calculated with the help of given formula:

$$H(x) = \sum_{i=1}^{N} P(xi) \log_2 \left(\frac{1}{pi}\right)$$

Where p (xi) the probability of event.

(d) Dempsters- Belief Theory

Dempster- Belief Theory is also called as Evidence theory or Theory of Belief Functions [6]. Recently, Belief theory, also known as Dempster-Shafer, or Evidence theory, has emerged as an important tool to manage and handle uncertainty and imprecision or even lack of information .This theory defines a sample space named frame of discernment (or simply frame), which is a finite set of mutually exclusive and exhaustive hypotheses in a problem domain under consideration. Dempster-Belief Theory is used to computes the probability that evidences support the attack or normal class .The use of Dempster Belief Theory steadily spreads out, mostly because it is used to cope with large amounts of uncertainties that are inherent of natural environments. This new approach considers sets of propositions and assigns to each of them an interval [*Belief, Plausibility*] [6].

In which the degree of belief must lie. Belief (usually denote Bel*)* measures the strength of the evidence in favour of a set of proposition. It ranges from 0 (including no evidence) to 1(denoting certainty).

Plausibility (*PI)* is denned to be

$$Pl(s) = 1 - Bel(\neg s)$$

Where ($\neg$s) is referring to its compliment "not s".

V. Conclusion

In this paper we proposed a new technique for intrusion detection that is based on one of the algorithm of Artificial immune system called The Dendritic Cell Algorithm (DCA) and The Dempster–Belief Theory (DBT) .With the help of Dempster–Belief Theory we calculate the degree of uncertainty and again on the basis of entropy calculated we find the intruder, having higher entropy, is regarded as the "intruder", and generate the alarm. With the help of dual detection technique we can not only minimize the false positive and false negative rate but also improved the correlation factor and decrease the intrusion rate in the system. So it is a better solution of intrusion detection. In this way we increase the security of the system more precisely and increase the efficiency of the system. However, since to the rate of classification is very large therefore the processing time is very long. Hence the future work is to minimize the processing time which can increases the efficiency of the system.

References

[1] Farhoud Hosseinpour, Kamalrulnizam Abu Bakar, Amir Hatami Hardoroudi, Nazaninsadat Kazazi, "Survey on Artificial Immune System as a Bio-inspired Technique for Anomaly Based Intrusion Detection Systems" 2010 International Conference on Intelligent Networking and Collaborative Systems, pp 158-189.

[2] P. Matzinger, "Tolerance, danger and the extended family," Annual Review in Immunology, vol. 12, pp. 991–1045, 1994.

[3] Debar H, Wespi A (2001), Aggregation and Correlation of Intrusion-Detection Alerts, the Fourth workshop on the Recent Advances in Intrusion Detection, LNCS 2212, pp 85-103.

[4] Dasgupta, "Immunity-based intrusion detection system: a general framework, Proceeding of the 22nd National Information Systems Security Conference (NISSC)", Arlington, Virgina, pp.147-160, 1999

[5] Matzinger. P, (1994) "Tolerance, Danger and the Extended Family", Annual Review in Immunology, vol.12, 2004, pp. 991-1045.

[6] G. Shafer, A Mathematical Theory of Evidence, Princeton, University Press, Princeton, NJ, 1976

[7] Aickelin U, Cayzer S (2002), "The Danger Theory and Its Application to AIS", 1st International Conference on AIS, 2002, pp. 141-148..

[8] Dasgupta and Gonzalez, "An Immunity-Based Technique to Characterize Intrusions in Computer Networks", IEEE Trans on Evolutionary Computation, pp.281-291, 2002.

[9] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using bayes estimators," in Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr. 2001.

[10] Guo Chen ,Peng Shuo ,Jiang Rong ,Luo Chao, "An anomaly detection system based on dendritic cell algorithm", 2009 Third International Conference on Genetic and Evolutionary Computing,pp192-195.