International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 6, Number 2 (April 2017), pp.20-30

http://www.meacse.org/ijcar

Negative Selection Algorithm: Recent Improvements and Its Application in Intrusion Detection System

Chikh Ramdane[1] and Salim Chikhi[2]

[1]Sétif 1 University, Sétif, Algeria

[2]MISC Laboratory, Constantine 2 University, Constantine, Algeria

Abstract

Negative Selection Algorithm (NSA) is the main method in Artificial Immune System (AIS). It was inspired by the self and non self discrimination behavior observed in the Mammalian Immune System (MIS). Since it emerged in the 1990s it has a great attention from researchers as a branch of bio-inspired computational intelligence. Due to its useful properties, it has been applied in different domains, and especially in the intrusion detection system (IDS). However, the basic version of NSA is still has many problems and poor performance on real applications, these limitations motivate researchers in this field to develop new models and variants for NSA. This paper introduces this paradigm and surveys the major and recent improvements in the NSA. Furthermore, a brief introduction to IDS is included with the NSA applications especially in IDS.

Keywords: Artificial Immune System (AIS), Negative Selection Algorithm (NSA), computational intelligence, Computer security, Intrusion detection System.

1. Introduction

Nature is an important source of inspiring the efficient solutions for a various problems. Mammalian Immune System (MIS) is an interesting source; it is a robust, distributed, multi- layered, adaptive, dynamic, and life-long learning system. The MIS is a complex network of tissues, organs, and chemicals. Its main function is to defend the body against foreign pathogens/antigens such as bacteria or viruses.

Artificial Immune System (AIS) can be defined as a computational system inspired by the principles and processes of the MIS, it uses ideas from the operation of the (MIS) and applies them to computational problems. Negative Selection algorithm (NSA) is one of the main algorithms in AIS. It simulates the immune tolerance in T-cell maturation process of biological immune system, and achieves effective recognition of non-self antigens by clearing self-reactive candidate detectors without any prior knowledge. The Researchers in this field focused on extracting and bringing the NSA features that would be advantageous to design an automatic solution for classification problems such as detection of computer intrusions.

However, the classical NSA is still suffers from many drawbacks such as: lacks continuous learning ability, generated detectors cannot completely cover the non self space, the time and space complexity, large number of detectors and a lot of redundant coverage between detectors. These limitations conduct researchers in this field to develop new models and variants that are more efficient than classical NSA. The remarkable ability of NSA to distinguish the difference between self (normal) and non-self (abnormal) have intrigued great interests in the computer security community and today, becomes one of the most mechanisms applied to intrusion detection.

This paper surveys the recent improvements of real NSA, shows its applications for IDS and aiming to provide useful information for NSA researchers about current developments and progress.

The paper is organized as follows. Section 2 presents the field of AIS focusing on NSA and summarizes the recent improvements and variants of NSA. Section 3 describes briefly the main components and the

most important aspects of IDS. When section 4 shows a list of recent works that combine NSA with IDS. The paper is concluded in Section 5.

2. Negative Selection Algorithm

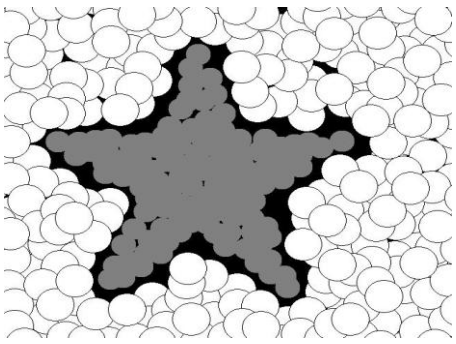
The artificial immune system (AIS) is a branch of bio-inspired and it has obtained a significant degree of success as a branch of Computational Intelligence since it emerged in the 1990s. An artificial immune system (AIS) uses ideas from the operation of the human immune system (HIS) and applies them to computational problems. A more detailed introduction of the HIS and AIS can be found elsewhere [27,32].

One of the interesting mechanisms of the adaptive immune system is the self/non-self recognition. The HIS is able to recognize which cells are its own (self) and which are foreign (non-self). Hence, it is able to build its defense against the attacker instead of self-destructing. Currently, the major types and the most popular theories of the AIS researches include Negative Selection Algorithm (NSA), clone selection , immune network theory , danger theory and positive selection , the NSA is one of the most applied and discussed model especially in intrusion detection.

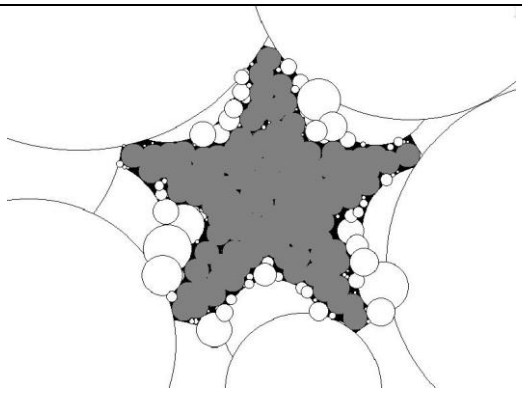
The NSA is the major algorithms of the AIS. It was inspired from the negative selection process of the adaptive immune system. The NSA has the capability to differentiate between the self-space (the cells, which are owned by the system) and non-self space (foreign entities to the system) which is obtained by T-cells, which are a set of non-self reactive detectors. NSA is firstly proposed by Forrest [27] which presents a framework to discriminate between self and non-self entities. This algorithm has a special characteristic that it needs only the normal samples in the training stage.

The classical NSAs consist of two stages [27]. Firstly, the NSAs generate a detectors set in the non self space. A candidate detector is generated in the whole space. If the detector does not match with the known self states, it becomes a mature detector and is added to the detector set. In the second stage, the unknown states are tested with the detector set. If an unknown state is matched by any mature detector, the NSAs assert that an anomaly occurs.

Fig. 1 illustrates the core idea of constant-sized and variable-sized detectors in 2-dimensional space. The grey area represents the self region, which is usually given through the training data (self samples). The white circles are the possible detectors covering the non-self region. "Holes" are illustrated in black. Fig. 1.a presents constant-sized NSA while Fig. 1.b illustrates the principles of variable-sized detectors.



a. NSA with constant-sized detectors



b. NSA with variable-sized detectors (V-detector)

Figure 1 Illustrates NSA in 2D-representation

2.1 Classification of NSA

There are a diverse family of NSAs has been developed, the essential characteristics of the original NSA introduced by Forrest [27] are still remaining. However the first NSA has large time cost complexity and space complexity. According to data representation there are two types of NSA: the binary NSAs(BNSAs) and the Real-Valued NSAs (RNSAs). Table1 presents a simple taxonomy of NSA.

NSA types / **Criteria's**	**Binary NSA[27]**	**Real NSA**	
		Constant-sized detectors	variable-sized detectors
Abbreviation	BNSA	CRNSA[18,28]	VRNSA(V-detectors)[13,21]
Data representation	Binary value (strings)	Real value	
Radius	Constant	Constant	Variable
Matching rules	r-contiguous bits(rcb), r-chunks, landscape-affinity matching, Hamming distance	Euclidian distances and its derivations	
Advantages	- Suitable for discrete space (representation and search) - Implementation simplicity	- High level representation, expressiveness and scalability	
		-	- Small number of detector - Best coverage of non self
Drawbacks	- The binary representation has some limitations for the real world problems	- The lack of continuous adaptability -Low detection rate and high false positive rate - Large time cost and space complexity	
		- Great number of detectors to cover the non self space - Great Overlapping between detectors	- Presence of the holes - some overlapping between detectors

Table 1 NSA classification

The algorithm of V-detector from [21] is the latest and most mature version. It took the most of advantages from the other versions and now is the framework for many researches. It was proposed by Zhou Ji and Dasgupta D.[21], The aim of authors is deal drawbacks of constant size detectors, in this algorithm, the size radii of detectors is change from one to others. Fig.2 represents the code of generation detectors of V-detectors.

Algorithm *V-detector NSA*
Input
S: Self set
r_s*: Self radii*
r_d*: detector radii*
c_0*: expected coverage*
T_{max}*: maximum number of detector*
$E=[0, 1]^n$ *: space state*
Output
D: Detector set
1: $D \leftarrow \emptyset$
2: ***repeat***
3: $t \leftarrow 0$
4: $T \leftarrow 0$
5: $r \leftarrow infinite$
6: $x \leftarrow$ *random sample from E*
7: ***repeat for every*** d_i ***in*** *D*
8: $dd \leftarrow$ *Euclidean distance between x and* d_i
9: ***if*** $d_d \leq r_d$ ***then***
10: $t \leftarrow t+1$
11: ***if*** $t \geq 1/(1-c0)$ ***then return*** *D*
12: ***go to*** *5*
13: ***repeat for every*** s_i *in S*
14: $d_s \leftarrow$ *Euclidean distance between x and* s_i
15: ***if*** $d_s - r_s \leq r$ ***then*** $r \leftarrow d_i - r_s$
16: ***if*** $r > r_s$ ***then*** $D \leftarrow D \cup \{< x, r>\}$ *where* $< x, r>$ *is a detector with location x and radius r*
17: ***else*** $T \leftarrow T+1$
18: ***if*** $T \geq 1/(1-$ *maximum self coverage)* ***then exit***
19: ***Until*** $/D/ = T_{max}$
20: ***return*** *D*

Figure 2 Detector generation algorithm of V-detector [21]

2.2 Recent improvements in NSA

Recently, many improvements of NSA have been proposed in the aim to overcome the limitations of classic version and most of them focused on the mechanisms of detector regeneration. However, satisfying detector coverage is still difficult to be realized. The authors in this field aim to show an improvement in the detection accuracy and algorithm efficiency, through covering a non self space with fewer detectors, and cover the holes by using detectors with a smaller radius. In the following, a list of new proposed models of NSA is presented:

ANSA [19] (2009). An improvement model of NSA named: A self-adaptive NSA which is referred as ANSA, is presented in [19]. The proposed NSA uses a novel technique to adjust adaptively the self radius and evolve the non self-covering detectors, to build an appropriate profile of the system only by using a subset of self samples. The aim of authors was to reduce the number of self elements and resolve the problem of adaptability in classical NSA. The experimental results on Iris data[31] show that ANSA is an efficient solution to anomaly detection and offers the characteristics of high detection rate, low false alarm rate, self-learning and adaptation.

EvoSeedRNSA[20] (2009). In order to improve the coverage of the non self space and generate an approximately optimal detector set a novel detector evolutionary generation algorithm for the Real-Valued Negative Selection Algorithm (RNSA) is proposed and termed as EvoSeedRNSA. The core idea of the EvoSeedRNSA is that it regards the detector set as a random sequence generated by some random seeds, and adopts a Genetic Algorithm (GA) to evolve the random seeds to acquire an efficient detector set. The experiments in the 2-dimensional synthetic data sets[21] demonstrate that the EvoSeedRNSA outperforms the traditional RNSAs and V-detector algorithm with a significant improved in detection rates and reducing in the number of mature detectors.

ORNSA [5] (2010). In this work, authors have proposed a novel NSA named Outlier Robust Negative Selection Algorithm (ORNSA) which uses an outlier robust and boundary detection technology to divide the selves into internal selves, boundary selves and outlier selves. Then, it combines the positive with negative mechanisms to cover non-self space more effectively. The biggest difference between ORNSA and traditional NSA occurs in the detection stage. The reverse detector set RD(r-detectors) and mature detector set MD (V-detectors) are both used during the detection stage. The experiment results in the synthesized data [21] and benchmark Fisher's Iris data[31] are used. Comparing with V-detector algorithm show that the new algorithm (ORNSA), has better adaptability and can obtain better detection performance by using fewer detectors. It also shows that the algorithm can deal with the training selves containing noisy data.

Optimized NSA [8] (2011). In NSA the problem of finding a good distribution of the detectors can be better stated as an optimization case. This work presents a new NSA using an optimization strategy base on re-heating simulated annealing algorithm; this algorithm modifies the position of randomly generated detectors to achieve optimal distribution without changing number of detectors. An optimal distribution consists to maximize the covering produced by a set of detectors, it is necessary to reduce their overlapping and not covering the self set. The proposed algorithm tested in 2-dimensional synthetic data [21]. Experiment results demonstrate that detection rate is improved and false alarming rate is decreased. Also, it applied for fault detection in analog circuit; result demonstrates that the proposed algorithm is better than artificial neural network.

FtNSA [16] (2012). An improved NSA by integrating a novel further training strategy into the training stage was proposed in [16], it named as FtNSA. The main process of this training strategy is generating self-detectors to cover the self region. A primary purpose of adopting further training is reducing self-samples to reduce computational cost in testing stage. It can also improve the self-region coverage. The experimental comparison among the proposed algorithm, the self-detector classification, and the V-detector on KDD CUP99[30] and 2-dimensional synthetic data sets[21]shows that the proposed algorithm can get the highest detection rate and the lowest false alarm rate in most cases.

IVRNSA [17] (2012). A new model of V-detector named IVRNSA was proposed in [17]. In the IVRNSA, every randomly generated candidate detector tolerates with detector set and becomes semi-mature detector when not matches with any existing mature detectors; the semi-mature detector outside of mature detectors' coverage self-tolerates with training set and becomes mature detector when not matches with any self element. The IVRNSA avoids the time-consuming self-tolerance process of candidate detector within the coverage of existing mature detectors, thus greatly reduces detector set size and significantly improves detector generation efficiency. The effectiveness and performance of IVRNSA algorithm is verified by a group of experiments. The experimental data includes the UCI Datasets [31]: Iris, Breast Cancer Wisconsin (BCW) and Synthetic Data Set (SDS)[21], show that the IVRNSA effectively improves detector generation efficiency and reduces time cost of algorithm.

CB-NSA[12] (2013). An improved NSA called CB-RNSA, which is based on the hierarchical clustering of self set, is proposed. In CB-RNSA, the self data is first preprocessed by hierarchical clustering, and then replaced by the self cluster centers to match with candidate detectors in order to reduce the distance calculation cost. During the detector generation process, the candidate detectors are restricted to the lower coverage space to reduce the detector redundancy. The theoretical analysis shows the time complexity of CB-RNSA is irrelevant to the self set size. Therefore, the difficult problem, in which the detector training cost is exponentially related to the size of self set in traditional NSAs, is resolved, and the efficiency of the detector generation under a big self set is also improved. The experimental results show that: under the same data set and expected coverage, the detection rate of CB-RNSA is higher than that of the classic NSA and V-detector algorithms. Moreover, the false alarm rate is lower than de same algorithms.

PRR-2NSA[9] (2013). The dual NSA based on pattern recognition receptors theory (PRR- 2NSA) is another model of NSA. The PRR-2NSA includes three separate stages, respectively: 1) the antigen clustering to generate APC classifier (self detectors) stage; 2) the negative selection process to generate T-cell classifier (detectors) stage; and 3) using the generated APC and T-cell Classifier to execute data classification stage. This mechanism can avoids the unnecessary and time-consuming self-tolerance process of candidate classifier within the coverage of existing mature classifiers, thus greatly reduces classifier set size, significantly improves classifier generation efficiency. Theoretical analysis and simulations on the classical UCI standard datasets[31]: "Iris" , "Breast Cancer Wisconsin Diagnostic" (BCW) and "Chess", show that the PRR-2NSA has better classifier set generation efficiency and lower false classification rate in comparison with V-Detector. Also, the PRR-2NSA can be applied in many two-class data classification applications, such as data classification, data mining, pattern recognition and network intrusion detection.

EvoSeedRNSAII [14] (2014). A modified EvoSeedRNSA, named as the EvoSeedRNSAII is proposed in[14] its aim is to overcome the shortage of the EvoSeedRNSA. An individual is represented by multi-group of random seeds. Different detector generation sequences are also discussed based on the new representation. The general frameworks of the EvoSeedRNSAII are the same as the EvoSeedRNSA. But, different from the EvoSeedRNSA, the EvoSeedRNSAII adopts a multi-group of random seeds to encode the individuals. The corresponding detector generation method for the individuals and genetic operators are also redesigned. The experiments demonstrate that the EvoSeedRNSAII has a better performance than the EvoSeedRNSA.

GF-RNSA [15] (2014). The real NSA based on the grid file of feature space (GF-RNSA) aims to improve the exponential worst-case complexity of existing NSA algorithms, and thus removes one major obstacle for applying negative selection to real-world problems. In the first stage of GF-RNSA, the n-dimensional feature space is divided into a number of grid cells, and then detectors are separately generated in each cell. As candidate detectors just need to compare with the self antigens located in the same cell rather than with the whole self set, the detector training can be more efficient. The experimental data includes KDD CUP99[30] and the Synthetic Data Set (SDS)[21] show that not only the time cost of negative selection, but also the time cost of data preprocess and detection are reduced, while the detection accuracy is not much declined.

NSA–DE [10] (2014). Is the name of an improved NSA using a differential evolution (DE) optimization. The uniqueness of this model is that the DE is implemented at the random generation phase of NSA; Local outlier factor (LOF) is implemented as fitness function to maximize the distance of generated spam detectors from the non-spam space. Validation of the proposed framework has been carried out with Spam dataset[22] and the results show that the detection accuracy of NSA–DE is better than the standard NSA model.

HNSA–IDSA [4] (2014). In this work, we have proposed and implemented a new NSA for Adaptive Network Intrusion Detection System it termed as HNSA–IDSA. The uniqueness of our model is that at the training stage of HNSA–IDSA the both type of data (normal and abnormal) are used to generate the normal and abnormal self detectors. In the testing stage of proposed NSA, the class of tested sample is determined by its position regarding to the normal and abnormal profile. This mechanism brings the adaptability and self-learning for proposed NSA. The experiment results in synthetic [21] and KDD99 [30] datasets show that HNSA-IDSA is an efficient solution to network intrusion detection and offer the characteristics of high detection rate, low positive false rate and adaptation.

NSA–PSO [7,1] (2014/2015). A new model that combines the NSA with particle swarm optimization (PSO) was proposed and implemented in [1,7]. The authors assumed that previous models have been limited by the adaptive nature of unsolicited email spam (non self). The researchers proposed an improved email detection system that is designed based on the combination between the real value NSA with particle swarm optimization (PSO). PSO was introduced to improve the random detector generation in the NSA. The combined NSA–PSO uses a local outlier factor (LOF) as the fitness function for the detector generation. The implementation and evaluation of the models are analyzed. This proposed technique can improve the traditional random generation of detectors in the real NSA and optimize the generated detectors in spam space at the same time. The results on datasets base Spam [22] show that the accuracy of the NSA–PSO model is better than the accuracy of the standard NSA model.

I-detector, OALI-detector [2] (2015). The independence problem between the training stage and testing stage of traditional NSA and the lack of continuous learning ability make its detector cannot completely cover the non self space. To overcome these problems a new NSA with online adaptive learning under small training samples (OALI-detector) was proposed and applied for anomaly detection. In this work a NSA named interface detector (I-detector) based on the boundary samples is presented, It can surround the self space with an appropriate self radius and carry out the learning process during the testing stage to adapt itself to real-time change of self space. The training stage of I-detector is to find the boundary samples. The experiments on 2-dimensional synthetic datasets and Iris data show that I-detector has high detection rate and high false alarm rate compared to other anomaly detection algorithms.

IO-RNSA [3] (2015). The main idea of immune optimization based real-valued NSA (IO-RNSA) is based on the distribution of self set in morphological space, and introduces the immune optimization mechanism, to produce candidate detectors hierarchically from far to near, with selves as the center, which decreases the redundancy between detectors and reduces the detection holes. Experimental results in 2-D synthetic data sets and three UCI datasets (Iris, Abalone and Breast Cancer Wisconsin Diagnostic) show that IO-RNSA has better time efficiency and generation quality than classical NSA, it also improves detection rate and decreases false alarm rate.

BIORV-NSA [6] (2015). In order to overcome some defects of original NSA such as: many “black holes” cannot be detected and excessive invalid detectors are generated. Lin C. *et al* [6] introduced a new NSA named bidirectional inhibition optimization r-variable NSA (BIORV-NSA). The proposed algorithm includes self set edge inhibition strategy and detector self-inhibition strategy. The first strategy defines a generalized radius for self individual area, making self individual radius dynamically be variable. While the second aims at mutual cross-coverage among mature detectors to eliminates those detectors that are recognized by other mature detectors and avoids the production of excessive invalid detectors. Experimental results using data sets from UCI [31] show that the proposed BIORV-NSA algorithm can cover more non self space, greatly improve the detection rates and obtain better detection performance by using fewer detectors.

NSA-II[29] (2016). In [29] an email detection system based on the modified classical NSA is proposed, it termed as NSA-II. The novel model improves the random generation of a detector in NSA with the use of both the spam and non-spam spaces. In the NSA-II training phase, two sets of detectors are generated; one for spam detectors and other for non-spam detectors. In testing phase, the detector outputs from the two sets are used. If one of the spam detectors make known new pattern, new email knows as a spam pattern. Otherwise, it considers as a non-spam pattern. The experimental results in spam base datasets [22] show that the detection performance of NSA-II is higher than the conventional NSA.

OALFB-NSA, FB-NSA [11] (2016). In the aim to bring the online adaptive learning ability to traditional NSA and extend its application range; a new NSA, named boundary-fixed NSA with online adaptive learning under small samples (OALFB-NSA) is proposed. In this work detectors are generated into two steps: In the first one the Boundary-fixed NSA (FB-NSA) generates a layer of detectors, which are around the self space. These detectors are only related to the training samples, and have nothing to do with the training times. In the second step OALFB-NSA detectors can adapt themselves to real-time variety of self space during the testing stage. Experimental comparison among proposed algorithms, V-detector and other anomaly detection algorithms on Iris datasets and biomedical dataset shows that the FB-NSA and OALFB-NSA can obtain the higher detection rate and lower false alarm rate in most cases.

2.3 Applications of NSA

Since his emergence, NSA has attracted the attention of many researchers and has been applied in numerous real world applications. Its development and application domains generally similar of those are of computational intelligence approaches such as artificial neural networks, evolutionary algorithms and fuzzy systems. In the following, a list of recent applications of NSA is presented: computer security [23,24], anomaly detection [2, 19, 28], data mining [33], optimization [34] and so on. In this work we will focus mainly in application the NSA for IDS.

3. Intrusion detection system

IDS is computer software designed to monitor an environment and identify the unauthorized access or the misuse of data. Nowadays, much attention has been paid to IDS which is closely linked to the safe use of network services and computer system. However, it is not possible to discern the attacks using only the preventive tools. So, IDS is considered as the complementary layer that can enhance the computer data security and detect new attacks.

Since its emerging in 90s, several of artificial intelligence methods and techniques have been used in aim to design a strong IDS. Such as[4]: ant colony optimization (ACO), particle swarm optimization (PSO), Fuzzy logic, K-nearest neighbor, Support vector machine (SVM), Artificial neural networks (ANN), Naïve Bays networks, decision tree, genetic algorithm, Hidden Markov models. For more explicit details of previous and current development, refer to the recent reviews [25, 26, 37]. Moreover, the IDS based on AIS becomes one of the focused topics in IDS researches. In this section we will interest only by IDS based NSA. The next paragraphs give a short highlight of some IDS aspects.

3.1 IDS architecture

In general, an IDS is based on the following modules:

- *Sniffer* or traffic Data Acquisition: This module is used in the data collection and responsible for extracting a set of selected features from captured traffic. In the case of a NIDS, the source of the data is rows of network frames or information from upper protocol layers (IP or UDP protocols).
- *Analyzer:* This module processes the data generated by the *Sniffer* module in order to identify intrusive activities. Once a malicious event has been detected, an alert will be raised and sent to the manager module.
- *Manager:* Once an alert is received, this module has the responsibility to initiate actions in response of a possible intrusion.

3.2 IDS taxonomy

There are a number of different ways to classify IDS. Here we focus only on the monitoring place and the analysis approach. According to the monitored environment, we can distinguish two types of an IDS:

- *Host-based intrusion detection system (HIDS*): HIDSs evaluate information found on a single or multiple host systems including files content of operating system and application.
- *Network-based intrusion detection system (NIDS):* NIDSs evaluate information captured from network communications or analyzing the stream of packets which travel across the network.

for a long time all IDSs are one of the two analysis approach[26]:

- *Misuse detection:* misuse detection uses pattern matching for the analysis, this approach examines network and system activities for known misuses, usually through some form of pattern-matching algorithm. The idea behind misuse detection consists of comparing network traffic against a model describing known attack. This approach has proved to be very effective at detecting known threats and it is generally favored in commercial products due to its predictability and high accuracy but largely ineffective at detecting unknown threats.
- *Anomaly detection:* This approach bases its decisions on a profile of normal network or computer system behavior, often constructed using statistical or machine learning techniques. Any event that does not conform to this profile is considered anomalous [25]. In academic research; this approach is typically conceived as a more powerful method due to its theoretical potential for recognizing novel attacks. However, its major drawback is a high false alarm rate**.**

3.3 Data Collection

In generally the data is collected one of from three sources: For NIDS, network traffic is collected using sniffer software like TCPDUMP data packets from networks. For HIDS, command sequences from user input or low-level system information, such as system call sequences, log files, and CPU/memory usage.

4. IDS based NSA

Due to its ability to distinguish the difference between self (normal) and non-self (abnormal), NSA fits naturally into the area of intrusion detection. Since its emergence in 90s, NSA is become one of the most mechanisms applied to intrusion detection. The Researchers in this field focus on extracting and bringing the NSA features that would be advantageous to design an efficient IDS and an automatic detection of computer intrusions. Here we summarized the most suitable NSA properties that are discussed by Kim and Bentley [23, 35] and Somayaji et al. [36]:

- NSA needs only Positive or normal sample in its training phase, these properties is very important in computer security because obtaining the normal data more easy and possible than obtaining abnormal data.
- Distribution: 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.
- Self-Organizing: a self- organizing IDS provides adaptability and global analysis. Without external management or maintenance, a self- organizing IDS automatically detects intrusion signatures (profile, pattern) which are previously unknown and/or distributed, and eliminates and/or repairs compromised components.

Nowadays, the IDSs based on IAS become one of the focus topics in IDS researches. Forrest et al [27], firstly use artificial immune method to protect computer. They viewed the problems of protecting computer system as distinguishing self from other. From Forrest [27] to now, tens of IDSs based NSA has been proposed and Implemented. Table 2 presents a list of works that combine IDS and NSA.

Author and year	IDS based NSA	Abbreviation	Testing datasets
M. Gong *et al* [16] (2012)	An efficient negative selection algorithm with further training for anomaly detection	FtNSA	KDD CUP99
Z. Sadghi and A. s. Bahrani s.b. [38] 2013	Improving the Speed of the Network Intrusion Detection	-	KDD CUP99
M. Mahboubian, N. A. W. A Hamid [39] (2013)	A Machine Learning Based AIS IDS	-	DARAP 1999 dataset
C. Ramdane and C. Salim[4] (2014)	A Hybrid new Negative Selection Algorithm for Network Intrusion Detection System adaptation	HNSA-IDSA	KDD CUP99
Ismaila I. *et al*[10] (2014)	new hybrid model combines Negative selection algorithm and differential evolution	NSA–DE	-Spam base dataset - E-mail spam
I. Idris *et al*[1] (2014)	Improved email spam detection model with negative selection algorithm and particle swarm optimization	NSA–PSO	-Spam base dataset -E-mail spam
I. Idris and A. Selamat. [7] (2015)	A combined negative selection algorithm with particle swarm optimization	NSA–PSO	-Spam base dataset -E-mail spam
O. Igbe *et al*[40] (2016)	Distributed Network Intrusion Detection System: An Artificial Immune System Approach	dNIDS	NSL-KDD

Table 2 IDSs based NSA

5. Conclusion

Negative selection algorithm is the main and the most applied algorithm in AIS. This is due to its ability to distinguish the difference between self (normal) and non-self (abnormal). Currently it attracting considerable interest from the research community and has several successful in real applications especially in intrusion detection system. In this paper we have firstly introduced AIS domain focusing mainly on real NSA, and then we summarized the recent improvements proposed by researchers for enhancing the efficiency of NSA and expanding its application area. Moreover, this paper investigated that NSA provides the useful properties for designing an efficient intrusion detection system. Finely, we hope that this survey can serve as a useful guide through the maze of the literature and highlight new research directions in AIS, in particular NSA.

6. References

[1] I. Idris., A. Selamat., Ngoc N. T. Nguyenc, S. Omatud, O. Krejcare, And K. Kucae, M. Penhakerf, "A combined negative selection algorithm–particle swarm optimization for an email spam detection system," In Engineering Applications of Artificial Intelligence Journal,vol.39, pp. 33–44, Elsevier, 2015.

[2] D. Li, S. Liu. and H. Zhang., "A negative selection algorithm with online adaptive learning under small samples for anomaly detection," In Neuro-computing Journal, vol. 149, pp. 515–525, Elsevier, 2015.

[3] X. Xiao, T. Li and R. Zhang., "An immune optimization based real-valued negative selection algorithm," in Applied Intelligence journal, vol. 42, pp. 289–302, ISSN 0924-669X (Print), 1573-7497 (Online), Springer, 2015.

[4] C. Ramdane. and S. Chikhi., " A New Negative Selection Algorithm for Adaptive Network Intrusion Detection System," in International Journal of Information Security and Privacy, vol. 8(4), pp.1-25, IGI Global, 2014.

[5] G. Li, T. Li, J. Zeng. and H. li, "An Outlier Robust Negative Selection Algorithm Inspired by Immune Suppression," journal of computers, ISSN: 1796203X, VOL. 5(9), academy publisher, 2010.

[6] L. Cui, D. Pi and C. Chen, "BIORV-NSA: Bidirectional inhibition optimization r-variable negative selection algorithm and its application," Applied Soft Computing, 1568-4946, (32)7, Elsevier, 2015.

[7] I. Idris and A. Selamat, Improved email spam detection model with negative selection algorithm and particle swarm optimization, "Applied Soft Computing, Vol. 22, pp.11–27, Elsevier, 2014.

[8] X. Aiqiang, L. Yong., Z. Xiuli, Y. Chunying and L. Tingjun, "Optimization and Application of Real-Valued Negative Selection Algorithm, " in Procedia Engineering, Vol.23, pp.241–246, Elsevier, 2011.

[9] X. Zheng., Y. Zhou. and Y. Fang, "Dual Negative Selection Algorithm based on Pattern Recognition Receptor theory and Its Application in Two-class Data Classification," In journal of computers, 1951-1959, vol.8, no. 8, academy publisher, 2013.

[10] I. Idris, A. Selamat. and S. Omatu," Hybrid email spam detection model with negative selection algorithm and differential evolution," in Engineering Applications of Artificial Intelligence, vol. 28, pp. 9 7–110, Elsevier ,2014.

[11] D. Li, S. Liu and H. Zhang, "A boundary-fixed negative selection algorithm with online adaptive learning under small samples for anomaly detection ," in Engineering Applications of Artificial Intelligence, vol. 50, pp. 93–105, Elsevier, 2016.

[12] W. Chen, T. Li, X. Liu and B. Zhang, "A negative selection algorithm based on hierarchical clustering of self set," in Information Sciences, vol.56, pp. 1–13, Science China and Springer-Verlag, 2013.

[13] Z. Ji and D. Dasgupta, "Real-valued negative selection algorithm with variable-sized detectors, " in Proceedings of the (GECCO-2004), Seattle, Washington, USA, , pp. 287–298, 2004

[14] J. Zhang and W. Luo, "EvoSeedRNSAII: An improved evolutionary algorithm for generating detectors in the real-valued Negative Selection Algorithms," Applied Soft Computing, 1568-4946, Elsevier, 2014.

[15] C. Wen, D. Xiaoming, L. Tao, Y. Tao, "Negative selection algorithm based on grid file of the feature space", Knowledge-Based Systems, 26–35, Vol.56, P. 26–35, Elsevier, 2014.

[16] M. Gong, Jian Z., J. Ma and L. Jiao, "An efficient negative selection algorithm with further training for anomaly detection", Knowledge-Based Systems, 185–191, Vol.30, P.185–191, Elsevier, 2012.

[17] P. Wu and X. Zheng, "An Improved Variable-radius Real-valued Negative Selection Algorithm", Journal of Information & Computational Science, 1548–7741, Vol.16, P.4713–4720, 2012.

[18] F. Gonzalez, D. Dasgupta and L. Fe. Niño, "A randomized real-valued negative selection algorithm, " (ICARIS-2003), Computer Science, v:2787, pp:261-272, Springer, 2003

[19] Z. Jinquan, L. Xiaojie, L. Tao, L. Caiming, P. Lingxi and S. Feixian, "A self-adaptive negative selection algorithm used for anomaly detection," in Progress in Natural Science, vol. 19, pp. 261–266, Elsevier, 2009.

[20] J. Zheng, W. Luo and B. Xu, " Generating an approximately optimal detector set by evolving random seeds," in The Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 978-0-7695-3929-4/09, IEEE ,2009.

[21] J. Zhou and D. Dasgupta, "V-detector: an efficient negative selection algorithm with“probably adequate” detector coverage, "Information Sciences, vol.179 (10), pp.1390–1406, Elsevier, 2009

[22] M. Hopkins, E. Reeber, G. Forman, S. Jaap: Spam Base Dataset. Hewlett-Packard Labs, 1999.

[23] J. W. Kim, "Integrating Artificial Immune Algorithms for Intrusion Detection," PhD thesis, University College London, 2002.

[24] B. Wang and S. Zhang, "A New Intrusion Detection Method Based on Artificial Immune System," In Network and Parallel Computing Workshops, pp.91-98, IEEE, 2007.

[25] S. X. Wu, W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review", Applied Soft Computing, vol.10, pp.1–35, Elsevier, 2010

[26] D. Dasgupta, S. Yu, F. Nino, "Recent advances in artificial immune systems," Applied Soft Computing, vol.11, pp.1574–1587, Elsevier, 2011.

[27] S. Forrest, A. S. Perelson, L. Allen and, R. Cherukuri, "Self non self discrimination in a computer," In PW IEEE Symp on Research in Securit and Privacy, IEEE, 1994

[28] F. Gonzàlez D. Dasgupta and R.Kozma, "Combining negative selection and classification techniques for anomaly detection," Proceedings of the Congress on Evolutionary Computation (CEC-2002), 0-7803-7282-4, IEEE, 2002.

[29] M. R. Abdolahnezhad, T. Banirosta, "Improved Negative Selection Algorithm for Email Spam Detection Application," in International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), ISSN: 2278 – 909X, Vol 5(4), 2016.

[30] Kddcup 99, http://archive.ics.uci.edu/ml/ datasets, 1999

[31] http://archive.ics.uci.edu/ml/machine-learning-databases

[32] L. N. De Castro and J. I. Timmis "Artificial immune systems as a novel soft computing paradigm, " Soft Computing,vol.7, pp.526-544, Springer, 2003

[33] M. Puteh, A.R. Hamdan, K. Omar and A.A. Bakar, " Flexible immune network recognition system for mining heterogeneous data," in 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008

[34] I.N. Vieira, B.S.L.P.d. Lima and B.P. Jacob," Optimization of steel catenary risers for offshore oil production using artificial immune system," in 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[35] J. Kim and P. Bentley,"The human immune system and network intrusion detection, ", In Proc. Of European Congress on Intelligent Techniques and Soft Computing (EUFIT '99), 1999.

[36] A. Somayaji, S. Hofmeyr, and S. Forrest, "Principles of a computer immune system", In Proc. of New Security Workshop, pages 75-82, Langdale, Cumbria, 1997.

[37] C. F. Tsai Y. Hsub, C. Linc and W. Lin, "Intrusion detection by machine learning: A review ", Expert Systems with Applications, 36, 11994–12000, 2009.

[38] Z. Sadghi and A. S. Bahrani," Improving the Speed of the Network Intrusion Detection," 5th Conference on Information and Knowledge Technology (IKT), IEEE, 2013.

[39] M. Mahboubian and N. A. W. A. Hamid, " A Machine Learning Based AIS IDS, ", International Journal of Machine Learning and Computing, Vol. 3, No. 3, June, 2013.

[40]O. Igbe, I. Darwish and T. Saadawi, " Distributed Network Intrusion Detection System: An Artificial Immune System Approach," IEEE First Conference on Connected Health: Applications, Systems and Engineering Technologies, IEEE, 2016.