Sudan University of Science and Technology

College of Engineering

Electronics Engineering Department

A Multi-Layer Network Defense System Based on Artificial Immune System

نظام متعدد الطبقات لحماية الشبكات مبني على نظام المناعة الاصطناعي

A Thesis Submitted In fulfilment of the Requirements for the Degree of Doctor of Philosophy in Electronic Engineering

Submitted By:

Mohamed Mohamed Khair Ellmubarak Elhaj

Supervised By:

Dr. Yahia Abdalla Mohamed Hamad

December, 2020

Sudan University of Science & Technology

College of Graduate Studies

جامعة السودان للعلوم والتكنولوجيا

كلية الدراسات العليا

كلية الدراسات العليا

Ref: SUST/ CGS/A11

Approval Page

(To be completed after the college council approval)

Name of Candidate: Mohamed Mohamed-khair ELMUBARAK ELHAJ

Thesis title: A Multi-layer Network Defense System Based on Artificial Immune System

Degree Examined for: PhD in Electronic Engineering

Approved by:

1. External Examiner

Name: IZZELDIN KAMIL AMIN

Signature: ..... Date: 16-12-2020

2. Internal Examiner

Name: ABUAGLA BABIKER MOHAMMED BABIKER

Signature: ..... Date: 16/12/2020

3. Supervisor

Name: Yahia Abdalla Mohamed

Signature: ..... Date: 16-12-2020

استهلال

قَالَ رَبِّ اشْرَحْ لِي صَدْرِي (*) وَيَسِّرْ لِي أَمْرِي (*) وَاحْلُلْ عُقْدَةً مِنْ لِسَانِي (*) يَفْقَهُوا قَوْلِي (*)

Acknowledgment

"In the name of Allah, most gracious, most merciful"

This thesis is dedicated to the soul of my father Mohamed Khair Elmubarak the one who formed my character and teach me how to face challenges and achieve my objectives.

I would like to thank my supervisor Dr. Yahia Abdalla and my former supervisor Dr. Mamoun Suliman and my co-supervisor Dr. Hussam Hamrawi for their wise guidance and support.

A very special thanks to all the members of my family specially my mother, my wife, my brothers and sisters and my uncle Basheir Hassan for their unconditional love, support, patience and encouragement.

I would also extend my gratitude and appreciation to my colleagues in TPRA and to the Sudan Emergency Response Team (Sudan CERT) and Nile Centre for Research and Technology for allowing my experiments to be conducted in their professional Labs.

Abstract

Artificial Immune System (AIS) is a promising computational intelligence system inspired by the biological immunity, it is a growing area of research attempts to bridge the divide between immunology and engineering, it exploits the mechanisms of the natural immune system including functions, principles and models in order to develop problem solving techniques. AIS offering great diversity of problem solving techniques and gaining increasing interest among researchers every day due to its powerful and diverse set of characteristics such as self-organisation, robustness, parallel distribution, feature extraction, diversity, learning, memory and adaptivity.

For decades computer and network security systems are facing a challenge of determining the difference between normal and potentially harmful activities. However, the nature of current and future threats in conjunction with ever larger and complicated IT systems urgently requires the development of automated and adaptive defensive tools. A promising solution is emerging in the form of hybrid security systems using biologically inspired computing, in particular artificial immune systems which inspired by the biological immune system detection and protection capabilities.

Inspired by many excellent characteristics of biological immune system, more and more computer security researchers integrate biological immune mechanisms into the network detection technologies, the network intrusion detection system (IDS) based on artificial immune system has become one of the focus areas of the intelligent research and achieved many good results in the recent studies.

The main contribution of this thesis is the work in progress to design and construct a hybrid intelligent multi-layered defence framework inspired by main AIS detection characteristics including its high abilities of dealing

with known and unknown attacks. The second major contribution of this project is the usage of fuzzy expert system for simulating innate immune system response motivated by its low solution cost for complex problems and the ability to translate uncertain expert knowledge into a decision-making process in a fast manner.

The proposed framework composed of two main layers using totally different strategies of detection and protection, which are innate and adaptive network defence components. The innate layer as first layer of defence designed and implemented using fuzzy logic expert system, and the adaptive layer as second layer designed using main immune system algorithms i.e. immune network algorithm, clonal selection algorithm and negative selection algorithm.

Results show the ability of the system to deal with about 80% of the traffic by the innate component with false positive rate of 1.7% and detection rate of about 97.79%, so the second layer will only deal with about 20% of traffic, this will reduce the overhead of the adaptive layer and the whole system. Results obtained from adaptive layer after co-stimulation check shows excellent results with false positive rate of only 0.78%.

This thesis also provides detailed review on AIS research focusing on the main frameworks which are considered as milestones in AIS research history, also provides suggestions extracted from deep study of different conceptual researches on how this rich research area can be improved and reach the equal importance and level of the other computational intelligence techniques.

المستخلص

نظام المناعة الاصطناعي هو أحد فروع أنظمة الذكاء الحسابي حيث يستلهم هذا النظام الخصائص المتفردة لنظام المناعة البيولوجي وهو نظام متطوّر يعمل على رأب الفجوة بين علمي المناعة والهندسة، ويستغل هذا النظام آليات نظام المناعة الطبيعية بما فيها المهام والمبادئ والنماذج لتطوير تقنيات قادرة على حل المشكلات المعقدة. نظام المناعة الاصطناعي يوفر تقنيات ذات تنوع كبير لحل المشكلات ويجد هذا النظام اهتماماً متزايداً من الباحثين يوماً بعد يوم بسبب مجموعة خواصه القوية والمتنوعة مثل التنظيم الذاتي والمتانة والتوزيع المتوازي وخاصية استخراج الخوّاص والتنوُّع والتعلُّم والذاكرة وقابلية التحكم.

لحقب متعددة واجهت أنظمة حماية الحواسيب والشبكات تحدياً هاماً تمثل في كيفية تحديد الفرق بين النشاطات الطبيعية والنشاطات الضارة في الشبكة، غير أن طبيعة المهددات الحالية والمستقبلية - آخذين في الاعتبار التعقيد غير المسبوق لأنظمة تكنلوجيا المعلومات - يتطلب بصورة عاجلة تطوير أدوات دفاعية ذاتية التحكم وتلقائية الاستجابة. أحد الحلول الواعدة والمستحدثة هو تطوير نظام أمن معلومات هجين بين الأنظمة التي تستلهم خواص الأنظمة الاحيائية وتحديداً نظام المناعة الاصطناعي الذي بدوره يستلهم خصائص الكشف والحماية من نظام المناعة الأحيائي.

المساهمة الأبرز لهذا البحث هي العمل الجاري لتصميم وبناء نظام دفاع هجين وذكي من طبقات دفاعية متعددة مستلهم من أبرز خصائص نظام المناعة الاصطناعي مع مقدرات كبيرة للتعامل مع الهجمات المعروفة وغير المعروفة. المساهمة الثانية الهامة للبحث تتمثل في استخدام نظام المنطق الضبابي لمحاكاة طريقة الاستجابة التي يقوم بها نظام المناعة الفطرية، وكان المحفز لاستخدام نظام المنطق الضبابي هو تكلفة حلوله المنخفضة عند استخدامه للمشكلات المعقدة ومقدرته على ترجمة المعارف والخبرات غير المرتبة الى اجراءات تؤدي الى قرارات واضحة وسريعة.

باستلهام كثير من الخصائص الممتازة لنظام المناعة الأحيائي، دمج كثير من الباحثين في مجال أمن الحاسوب آليات نظام المناعة الأحيائي في تكنولوجيات حماية الشبكات، فأصبح نظام كشف الاختراقات في الشبكات المبني على نظام المناعة الاصطناعي، أصبح من المجالات المركّز عليها من قبل الباحثين في مجال الذكاء الصناعي وتوصلت لنتائج جيدة في الدراسات الحديثة.

الاطار المقترح يتكون من طبقتين رئيسيتين تستخدمان استراتيجيتين دفاعيتين مختلفتين تماماً، طبقة تمثل المناعة الأولية أو الفطرية وأخرى تمثل المناعة المكتسبة أو المتكيّفة. الطبقة التي تمثل المناعة الفطرية كطبقة أولى للدفاع صممت ونفذت باستخدام نظام المنطق الضبابي، أما الطبقة

التي تمثل المناعة المكتسبة كطبقة ثانية للدفاع صممت باستخدام خوارزميات رئيسية من نظام المناعة الاصطناعي مثل خوارزمية شبكة المناعة وخوارزمية اختيار النسل وخوارزمية الاختيار السلبي.

نتائج الاختبارات أظهرت مقدرة النظام على التعامل مع حوالي 80% من الحركة بالشبكة بواسطة المكوّن الذي يمثل المناعة الفطرية مع معدل خطأ ايجابي حوالي 1.7% ونسبة كشف للمهددات بلغت حوالي 97.79%، وهذا يعني أن الطبقة الثانية ستتعامل فقط مع حوالي 20% من الحركة، هذا الأمر سيقلل الضغط على نظام المناعة المكتسبة وبالتالي على النظام ككل. اختبارات الطبقة الخاصة بالمناعة المكتسبة بعد اضافة خاصية الاشارة الثانية أوضحت نتائج ممتازة مع معدل خطأ ايجابي يبلغ فقط 0.78%.

هذا البحث يقدم أيضاً مراجعة مفصّلة عن البحوث الخاصة بنظام المناعة الاصطناعي بالتركيز على الأطر الرئيسية التي تعتبر كبحوث أساسية ومرجعية ومعلماً في تاريخ البحوث الخاصة بهذا العلم، ويقدم البحث أيضاً مقترحات مستخلصة من دراسة عميقة لبحوث مفاهيمية مختلفة لكيفية تحسين البحث الخاص بهذا المجال الغني وكيفية الوصول به لدرجة متساوية في الأهمية والمستوى مع تقنيات الذكاء الحسابي الأخرى.

Table of Contents

Chapter Three: Human Immune System

Chapter Four: A Novel AIS Framework for Network Security

List of Figures

List of Tables

Abbreviations

Ab	Antibody
ABM	Agents Based Model
Ag	Antigen
AI	Artificial Intelligence
AIN (aiNet)	Artificial Immune Network
AIS	Artificial Immune System
ANN	Artificial Neural Networks
APC	Antigen Presenting Cells
AUC	Area Under Curve
B-Cell	B-Lymphocytes
BIS	Biological Immune System
CI	Computational Intelligence
CID	Intrusion Detection Capability
CPE	Cost Per Example
CSA	Clonal Selection Algorithm
DCA	Dendritic Cell Algorithm
DDoS	Distributed Denial of Service
DoS	Denial of Service
DT	Danger Theory
FLS	Fuzzy Logic System
FM	F-measure
FNR	False Negative Rate
FPR	False Positive Rate
GA	Genetic Algorithm
HIDS	Host-based Intrusion Detection System
HIS	Human Immune System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IPS	Intrusion Protection System
INT	Immune Network Theory
IT	Information Technology
MHC	Major Histocompatibility Complex
NIDS	Network-based Intrusion Detection System
NIS	Natural Immune System
NK	Neural Killer Cells
NSA	Negative Selection Algorithm
NSA	Negative Selection Algorithm

PHP	Hypertext Preprocessor
PRR	Pattern Recognition Receptor
PSA	Positive Selection Algorithm
R2L	Remote to Local
SVM	Support Vector Machine
T-Cell	T-Lymphocytes
Th	T helper cells
TNR	True Negative Rate
TPR	True Positive Rate
U2R	User to Root

CHAPTER ONE

INTRODUCTION

1. Introduction

3.1 Background

Artificial immune system is a promising computational intelligence system inspired by human immune system which acts as natural resistance to diseases using sophisticated mechanisms intended to protect human bodies from invaders. AIS has been around for decades, it emulates those of humans in order to solve complex problems. Constructing computational intelligent solutions inspired by natural systems is not a new idea, neural networks and evolutionary computation are good examples of those kind of systems that interest many researchers [1, 2, 3]. AIS as computational intelligence system is inspired by human immune system which has several properties of real interest for researchers such as uniqueness, anomaly detection, noise tolerance, distributed detection, learning and memory [4, 5, 6, 7]. AIS research has been applied to solve complex computational and engineering problems related to several applications especially in classification, optimization or anomaly detection [8].

On the other hand, network security systems like IDS/IPS, antivirus, anti-malware and firewall are not looking sufficient in stopping the harms that new sophisticated networks are suffering these days from ever evolving attacks and malicious activities.

One of the most common applications applied in AIS research is network security due to the characteristic similarities between attacks on computer networks and on human organs. High similarities have been noticed between the biological immune system in human bodies and the network security system in computer networks since both are intended to protect against attacks and prevent from invaders [6].

Most AIS research focused on the adaptive component and only recently the innate component has been introduced. Many applications and

frameworks using adaptive immune mechanisms are available in literature, and in contrast innate mechanisms can hardly be found.

In this thesis results show that incorporating properties of biological innate immune system into artificial immune system in computer security applications lead to very effective systems and perform better than systems with only adaptive immunity [9]. This thesis agrees with the proved hypothesis that the innate immunity is largely responsible for controlling and directing adaptive response [1]. Therefore, the system is highly depends on the interaction between the innate and adaptive subsystems.

Throughout literature it can easily be noticed the great achievements that AIS has accomplished, while still there is big room of improvement and development for AIS algorithms and models [10].

Hybrid systems are growing computational intelligent areas, in these systems various intelligent methods and techniques like neural networks, fuzzy logic systems, artificial immune systems, evolutionary computation, and genetic algorithms are combined together in a single system. AIS, as well, when combined with other computational intelligent systems will benefit from this combination by adding more techniques, algorithms and inspiration to the new combined system [10].

This thesis presents a research that designs, models, implements and tests a new multi-layered computational intelligence network defence framework based on Artificial Immune System (AIS).

3.1 Problem Statement

Modern societies have become dependent more than anytime on information and communication technology (ICT), this dependency lead to an increasing number of risks and threats. On one hand, the Internet is becoming an important tool and an integral part of daily life, and overall reliance on the Internet is increasing every day. On the other hand,

information technology tools and techniques have become more proficient, effective and economical over time, and at the same time malicious tools and techniques have become more professional and sophisticated.

When investigating methods of IDS/IPS it is noticed that these solutions have some real drawbacks, such as high false positive rate, inability to deal with unknown patterns, the need to manually update signature database and inability to detect new threats [11, 12]. And when looking to the management side it is important for the IDS to be simple, efficient and not using too many resources although it is tasked to read and assess many events, bugs and logs. Furthermore, it is well known that detecting intrusions in a network environment is a very challenging task due to the big number of communication protocols, increasing number of operating systems, services, applications, vulnerabilities, bugs, errors, etc [13].

So current detection and protection capabilities are facing complicated difficulties which require in-depth, intelligent, effective and comprehensive network defence solutions that this research is aiming to develop.

This thesis is intended to make use of the useful ideas from human immune system to build an effective defence mechanism able to protect computer networks, so it explored properties, algorithms and applications of AIS. It investigated and explored human immune system ways of protection like multi-layered defence strategy and addressed innate immunity central role in AIS. The research main assumption is that by incorporating properties of biological innate immunity into AIS, the performance of artificial immune system can be enhanced.

Correspondingly, it is assumed that integrating different computational intelligence techniques like AIS and fuzzy logic system shall help to overcome individual limitations through the combination of different

techniques. This integration has notably contributed in the developments of new effective intelligent systems [10].

The immune system generally intended to protect human body from harmful entities that are for the most cases foreign entities, but in some cases, damage could be originated from inside, which is considered one of the main challenges facing protection systems [14]. The proposed system should also be capable of learning by itself and update automatically without human interaction.

In modelling effective adaptive immune system, this research faced another challenge of constructing millions of antibodies and antigens, building enough number of antibodies consuming numerous storage and processing resources [13].

In the tests conducted in this proposed framework, KDD'99 dataset is used which is a benchmark dataset well defined, organized and labelled to precisely evaluate the performance of intrusion detection/protection systems. This dataset has inherent problems, it is imbalance since two attacks made more than 70% of the whole dataset, it is outdated and contains many duplicated connections [15, 16].

Another important challenge, was to find solutions to the drawbacks associated with the algorithms used in this research like complexity and high false positive rate problems in negative selection algorithm [17].

3.1 Research Objectives

In this thesis and based on AIS theory, a new network security framework is presented, the thesis describes the detailed steps taken to model and implement a multilayer network defence system using artificial immune system theory, the main objectives of this research are:

A- Modelling the behaviour of human immune system by designing an AIS with algorithms capable of detecting efficiently intrusions in a network environment;

B- Develop intrusion detection capabilities that able to overcome well known IDS limitations;

C- Integrating different computational intelligent techniques to overcome individual limitations and enrich network defence system through combining different intelligent techniques;

D- Build in-depth adaptable security mechanisms capable of learning by themselves and defend network from inside and outside attacks.

3.1 Proposed Solution

The solution proposed in this research are based on a comprehensive study and a detailed analysis to both network security solutions and AIS theories and algorithms. The proposed system composes of two main layers, innate and adaptive layers. The innate layer as a first layer of defence is designed and implemented using fuzzy logic expert system. The adaptive layer as a second layer is using typical adaptive immunity algorithms. This thesis shows detailed description of the framework and results from the whole system.

The proposed innate layer response highly reflects the properties of the human innate system in responding to antigen stimulus actions, it is the first layer to generate response to antigen entering human body so it is the first responder to invaders and first layer that defend human body, it is also designed to classify attacks according to general properties and to network behaviour. The system deals with non-fuzzy inputs, in the form of network connections, as well as uncertain ones using fuzzy expert system abilities to translate uncertain expert knowledge base into a decision-making process and its known capabilities of converting human rules into mathematical formulations to be easily designed and implemented using computer programs.

The adaptive layer is designed to simulate the adaptive immune functionality of responding to individual attacks in a specific manner and using memory cells to better respond next time once encountering the

same attack. This layer is designed and implemented using well known AIS algorithms like negative selection algorithm, clonal selection algorithm and immune network algorithm.

3.1 Methodology

As illustrated in Figure 1.1 bellow, the methodology used in this research are composed of four consecutive steps starting from studying and analysing the two main parts of the research, the network security and immune system theory. Then designing and developing a suitable system based on the ideas and gaps collected during step 1, then constructing the designed framework, and last conducting the experiments and tests to verify and validate the concepts used.

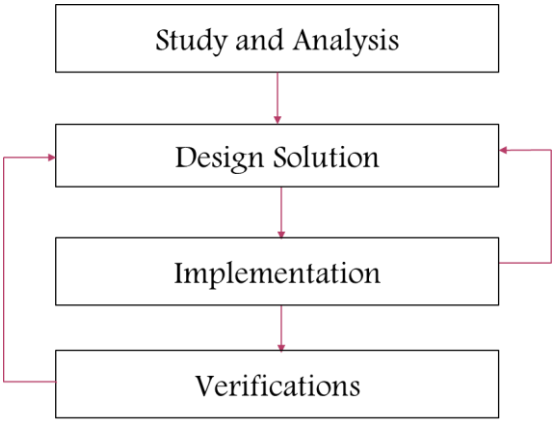


Figure 1.1. Research methodology used

1- Step 1: Study and analysis main components of the system:

In this early stage two main studies followed by a deep and precise analysis to both network security and artificial immune system took place. The first study conducted was started by an investigation on network security with special concentration on IDS. IDS types, capabilities, limitations, challenges and roles were studied, this include the difficulties facing all other types of network security devices and software like antivirus, firewall, anti-spam, anti-malware and others. In this research there was an obvious need to study the behaviour of network and computer attacks in a complicated network environment,

this study was taken place for different kind of attacks and for abnormal activities.

The second study conducted in this stage related to artificial immune system and the capabilities, characteristics, theories, applications, algorithms and frameworks of the human immune system with special focus on the detection and protection capabilities that may be inspired solutions to network security issues.

These two comprehensive studies were followed by a very concentrated analysis to find best solution based on AIS theory to network security issues, this solution should be intelligent, robust, comprehensive, adaptable, multi-layered, manageable, cooperative and with in-depth detection and protection capabilities. The analysis also extracted the main gaps that this research should fill, like:

- Researchers are focusing on inspiring solutions to engineering problems from adaptive immune system although innate immunity are essential part of the immune system and can enhance the overall performance when incorporated with adaptive immunity;
- IDS as an important part of any modern network has known limitations and difficulties especially when facing unknown attacks;
- Instead of having multiple devices to security problem in a sophisticated network, it is decided to have one smart solution, so the research is focused on building one single multi-layered and adaptive defence system inspired by immune system protection capabilities.

2- Step 2 – Designing and modelling suitable solution:

At this stage all information gathered and analysed at step one are taken into account for building a framework defined in the proposed solution above. At step two there are five tasks took place as follow:

a) Define the characteristics of multilayer immune systems: AIS as an adaptable system inspired by human immune system which is well-known with its notable abilities of learning, recognition and characteristic extraction, it is also parallel, distributed, adaptive and self-organizing system to name some of its important features. Those characteristics should be further explored in this stage to better understand the added value of AIS to the field of computational intelligence and in solving complex engineering problems. Similar to all researches of biological inspired computational intelligence techniques, this research is intended to extract ideas and algorithms from biological immune system in order to develop models and tools able to solve complex engineering problems such as network defence. In this research, a layer-based defence capability is studied to formulate a multilayer computer network defence system inspired by biological immune theories and algorithms, the main two layers identified in this system are innate and adaptive components. The characteristics of multilayer are properly defined in nature, especially in human immune systems, the proposed solution attempt to utilise the most important capabilities of the natural immune system while the lack of serious attempts for innate immunity modelling in literature were highlighted.

b) Define characteristics of innate immunity: How researchers develop their investigation from using only adaptive immunity to recent researches incorporating innate immunity as well, are explored in this stage. Furthermore, identification is built on research by biologists identifying the characteristics of innate immunity in humans. Research also indicated that clear desirable characteristics from innate immunity for network

defence are justified. These characteristics are clearly stated and formulated the bases for choosing appropriate algorithms to model the behaviour of an innate immune system.

c) Develop a multilayer framework: In this stage the complete frame work is developed according to the characteristics defined for a proper multilayer system used for network defence. These characteristics are mapped to build a multilayer AIS capable of performing well or better than legacy single layer AIS (i.e. adaptive only systems) or multilayer AIS frameworks that use adaptive and algorithms other than fuzzy logic for innate immunity layer.

d) Develop innate layer algorithm: The innate layer is modelled and designed using fuzzy expert system. The immune system is built based on the characteristics identified relating to desirable behaviour of the system, in which fuzzy expert systems are found to be most suitable. The suitability of the fuzzy system is confirmed by studying the behaviour of such systems in the extensive applications in the literature, and with proper study of its performance. The design consists of constructing the building blocks of the fuzzy rule-based system. The typical fuzzy system needs to define the linguistic variables and their rules from the network data and network experts. The knowledge base and the method of defuzzification were designed and chosen in this stage.

e) Choose adaptive layer algorithms: In literature review an investigation to innate and adaptive layers of defence, their algorithms, tools and usage took place. The theoretical aspects of this field are yet to grow and its applications are numerously starting to escalate, which gives indications of the fields potential in providing solutions that are comparably efficient and

viable. The adaptive layer is modelled and designed using main adaptive immunity algorithms. These algorithms are proven to have reasonable results based on previous studies and are well documented in the literature.

3- Step 3 - Assemble the entire system:

Here in this stage a comprehensive framework that was modelled in step two above were constructed. During the implementation phase there was a need to modify and enhance the designed solution. So, the two layers of defence were built to work independently, but still in a cooperative way. The framework at this stage is entirely coupled to perform its task in network defence and ready for validation and testing.

Step 4 - Design experiments for validation:

In this research the algorithms required to accommodate the solution to a multilayer network security application using AIS are formulated, tested for applicability, and evaluated comparatively with existing methods. The developed systems are tested and evaluated for accuracy and computational complexity in this stage. The outcome of the research should arrive at identifying the type of problems that a typical method of AIS is likely to be used for, and to address and develop an understanding of any performance differences. Appropriate software and simulations are developed for evaluation and demonstration. Last, to test the system well-known dataset i.e., KDD'99 dataset. The different types of datasets are investigated and then compared in order to justify the use of this dataset with all its drawbacks. These drawbacks are properly studied and some measures have been identified to overcome these limitations. In this stage tests are performed by the system and extensive studies and comparisons are made for the performance and conclusions are drawn.

3.1 Research Outlines

In chapter two a literature review on artificial immune system generally including its algorithms and applications is provided, this survey reflects

what other researchers find out and how do they progress. This chapter provided an introductory information on AIS theory beside a deep analysis on the research of AIS generally. Then the same chapter investigated and described other components of this research including network security with special focus on IDS and fuzzy logic system.

Chapter three presented human immune system characteristics and the way of protecting human body, this include layers of defence and general algorithms and theories.

Chapter four described the general framework proposed by this research and explored its mechanisms and theories. The two main components used in the framework were described in details.

In chapter five experiments results are explored, then the thesis concluded with chapter six which provided summary to the thesis beside main contributions and possible future work.

Figure 1.2 below presents the entire thesis structure.

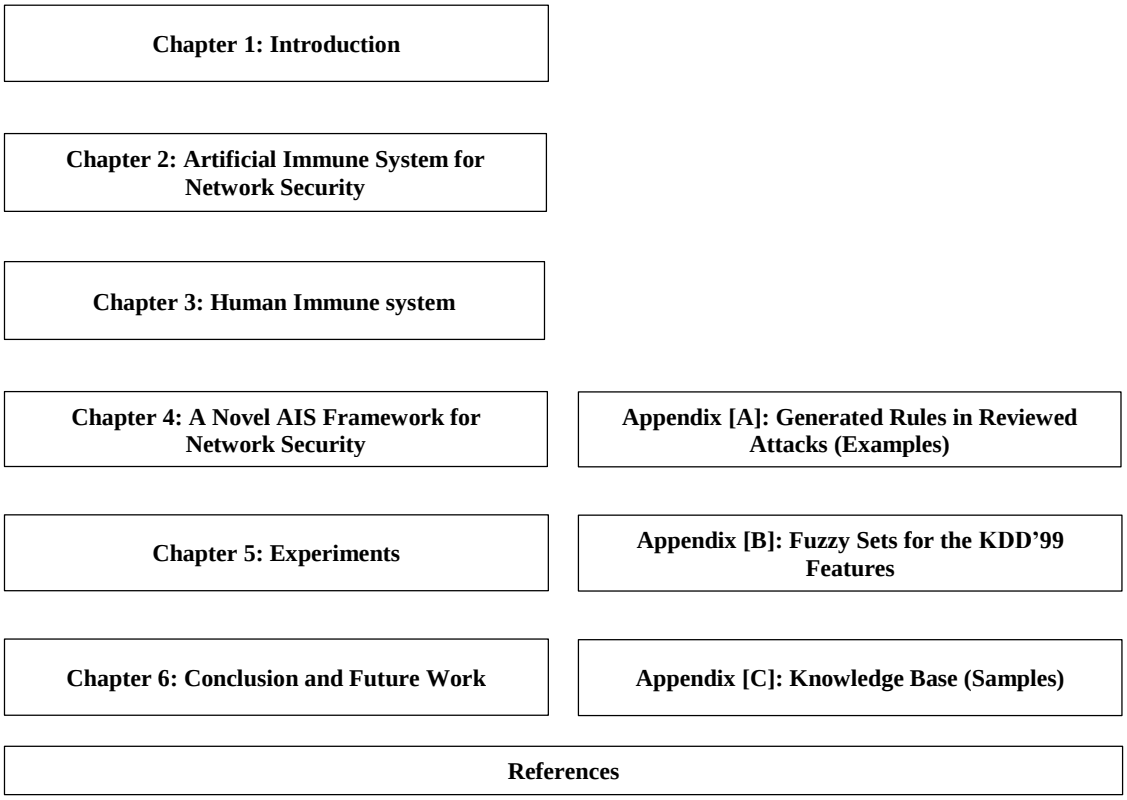


Figure 1.2. Thesis Structure

CHAPTER TWO

ARTIFICIAL IMMUNE SYSTEM FOR NETWORK SECURITY

2. Artificial Immune System for Network Security

2.1 Overview

This chapter reviews artificial immune system (AIS) as a computational intelligence technique inspired by biological immune system and provides literature review on the biological inspired systems used to solve complex engineering problems then provides an insight to network security solutions using AIS theory.

Section two introduces the computational intelligence concept and shows its main differences with artificial intelligence system. Section three presents in details the hybrid intelligent systems where researchers tend to solve real problems by combining two or more intelligent systems to overcome individual limitations. Section four defines AIS and reviews this important research domain showing the progress and success achieved, and also shows the drawbacks and limitations then extracted suggestions on the way forward from literature.

Section five and six provide detailed information on applications and properties of AIS and human immune system that convinced researchers to design solutions inspired by biological immune system to problems that are difficult to solve using traditional methods.

Section seven describes the similarities between AIS and network security capabilities and shows the ways to map AIS with IDS and network attributes. Section eight introduces IDS as an important element of today's networks and describes its structure, types and defence mechanisms and its different placing options in the network. Section nine presents a detailed review on network security and IDS applications inspired by human immune mechanisms and theories. The last section of this chapter introduces the fuzzy logic system as a computational intelligent system and presents a detailed review on the use of fuzzy logic systems with IDS and AIS.

2.2 Computational Intelligence Systems

2.2.1 Computational Intelligence Techniques Inspired by Nature

Researchers have defined the term computational intelligence (CI), since it was first introduced in 1990 by the IEEE Neural Networks Council, in tens of research papers but still no commonly accepted and adapted definition yet [3]. In the other hand, IEEE Neural Networks Council defines artificial intelligence as "a study of how to make computers do things at which people are doing better" [2].

The first known definition of computational intelligence was by Bezdek [18] as a system first dealing with low level data such as numerical data and does not use knowledge in the artificial intelligent sense, and when it begins to exhibit computational adaptivity, fault tolerance, speed approaching human-like turnaround and error rates that approximate human performance [18].

Other definition proposed and argues by some researchers is that computational intelligence is a collection of heuristic techniques such as swarm intelligence, fractals, chaos theory and immune systems. Meanwhile, some researchers see no differences between computational intelligence and artificial intelligence techniques and both have same goals. Based on different levels of analysis of system complexity, Bezdek [18] sees computational intelligence as a subset of artificial intelligence [3]. Engelbrecht [2] concentrates on computational intelligence as a sub-branch of artificial intelligence and defines it as an adaptive mechanism facilitates intelligent behaviour in complex and changing environments.

Looking closely to the modelling and designing research related to solving real-live problems it can easily be concluded that in the near future human knowledge will become more important in system modelling as a suitable replacement to classical mathematical modelling. Those systems based on human knowledge are called computational intelligence systems according to Siddique [3] and the team.

In the last few years, a great increase in interest in modelling computational intelligence systems inspired by nature could perceived particularly from human biology which clearly has achieved notable success, among these systems artificial neural networks, DNA computation, evolutionary algorithms, swarm intelligence, artificial immune systems and fuzzy logic systems [2, 3, 5, 19].

Biology over years is considered a rich source of inspiration for modelling and designing solutions to real world complex problems. In fact, creating intelligent systems and non-traditional approaches inspired by nature and biology has been of interest to scientists and researchers for quite long time. Meanwhile, it is clearly recognized that it is not possible to mathematically model all engineering and real world problems [3, 19, 20]. Nature/bio-inspired techniques have proved their usefulness and efficiency in solving complex research problems. For instance, genetic algorithm (GA); a metaheuristic evolutionary algorithm inspired by the process of natural selection, have been successfully used to solve optimization problems. In addition to being used in optimization, bio-inspired techniques like GA and artificial neural networks (ANN) have been successfully applied to the areas of data classification, clustering and anomaly detection [21]. Bio-inspired algorithms and techniques are developed not as a means of simulation, but because they have been inspired by the key properties of the natural system. The algorithms attempt to improve computational techniques by mimicking successful natural phenomena, with the goal of achieving similar desirable properties as the natural system [12].

2.2.2 Hybrid Intelligent Systems

As stated in the previous section computational intelligence techniques have shown notable success recently when applying single technique at a time, but it is proved that modelling hybrid systems working cooperatively is more effective in solving complex real world problems. Integrating

different learning and adaptation techniques is very useful for overcoming individual limitations and weaknesses. This trend is one of the most intensively growing areas in recent years, and it has contributed effectively in the developments of a large number of intelligent system designs [2, 10, 22, 23].

Hybrid intelligent systems utilize the main characteristics of various soft computing methods and techniques like artificial neural networks, fuzzy logic system, artificial immune systems, evolutionary computation and genetic algorithms [10, 22].

Researchers generally have explored combining two different computational intelligent techniques, in literature many examples can be found of models with this combination providing solutions to a very complex real world problems.

Researchers also observed that AIS are incredibly flexible, as are many biologically inspired techniques, suitable for a number of applications and can be thought of as a novel soft computing paradigm, suitable for integration with many more traditional techniques. Table 2.1 below gives examples of combining AIS with other computational intelligence systems.

Table 2.1. Combining AIS with other computational intelligence systems - review

Reference	Main idea of the research
Hajela et al., 1997 [24]	Some of the earlier work that combined AIS ideas with genetic algorithms. Immune networks is used to improve the convergence of genetic algorithms.
Nasaroui et al., 2002 [25]	Proposed the Fuzzy AIS model, which uses a fuzzy set to model the area of influence of each B-cell, which makes it more robust to noise.
Vargas et al., 2003 [26]	Presented an immune learning classifier network named CLARINET for autonomous navigation by combining the strengths of learning classifier systems, evolutionary algorithms, and an immune network model.
Xian et al., 2005 [27]	Proposed a novel intrusion detection method that optimizes the objective function of unsupervised fuzzy k-means clustering based on clonal selection algorithm.
Karakasis & Stafylopatis, 2006 [28]	Introduced a hybrid technique for data mining tasks which combines clonal selection principles and gene expression programming.

Fu et al., 2007 [29]	Proposed a hybrid artificial immune network which uses the swarm learning of particle swarm optimization to speed up the convergence of artificial immune system.
Gan et al., 2007 [30]	Proposed a technique that combines the simple representation method of gene expression programming and the advantage of clonal selection algorithms.
Danzhen et al., 2008 [31]	Introduced a fuzzy artificial immune network (FaiNet) algorithm for load classification. It consists of three parts: the artificial immune network learning algorithm, the minimal spanning tree algorithm, and the classification algorithm based on fuzzy C-means algorithm [10].
Neal et al., 2005 [32]	The proposed system combined the algorithms of three intelligent systems, which are: artificial immune system, artificial neural system and artificial endocrine system. The proposed model is intended to use as a control system for complex electronic and electromechanical systems that would profit from long term autonomous operation.
Mu-Chun Su et al., 2008 [11]	Presented an on-line learning neuro-fuzzy system which was inspired by the metaphor of biological immune systems. It illustrates how an on-line learning neuro-fuzzy system can capture the basic elements of the immune system and exhibit some of its appealing properties.
Bateni et al., 2013 [33]	In this research a new automated alert correlation approach is presented. It employs Fuzzy Logic and artificial immune system to discover and learn the degree of correlation between two alerts and uses this knowledge to extract the attack scenarios.
Sanyal & Thakur, 2012 [34]	The suggested hybrid approach based on artificial immune system and Soft Computing is instrumental in detecting intrusions and malicious activities in a given network. The three primary components of the system: surface barrier, innate immune system and adaptive system provide a multi-layered defence mechanism, which evolves over multiple executions to combat new emerging attacks.
Shamshirband et al., 2014 [35]	A bio-inspired method is introduced, namely the cooperative based fuzzy artificial immune system (Co-FAIS). It is a modular based defence strategy derived from the danger theory of the human immune system. The agents synchronize and work with one another to calculate the abnormality of sensor behaviour in terms of context antigen value (CAV) or attackers and update the fuzzy activation threshold for security response.
Shin & Kuan, 2008 [36]	This work proposed an evolutionary multi-objective optimization algorithm that applies the concept of biological immune system as an alternative algorithm for solving Pareto engineering optimization problems. The optimization algorithm developed and presented in this research uses the cycle of affinity-maturation principle in the immune system that contains the repeated activation, proliferation and differentiation.
Yang Liu, 2009 [37]	This thesis proposed a bio-inspired computational framework, the Neuro-Immune Network reGulating (NING) framework. A machine visual tracking system is created to characterize and parameterize the NING framework.
Obinna Igbe, 2019 [21]	This thesis showed how the success of applying a combination of ANN and AIS to intrusion detection with great detection accuracy. With the drawback being the enormous time it takes to train an ANN.

2.3 Artificial Immune System (AIS) - Definition

As illustrated in Figure 2.1 below, artificial immune system is a relatively new branch of computational intelligence technique offer powerful and robust information processing capabilities, it is steadily progressing technique inspired by biological immune system, this reflects the increasing interest of researchers to inspired solutions for difficult and complex computational or engineering problems from nature [38, 39, 40, 41].

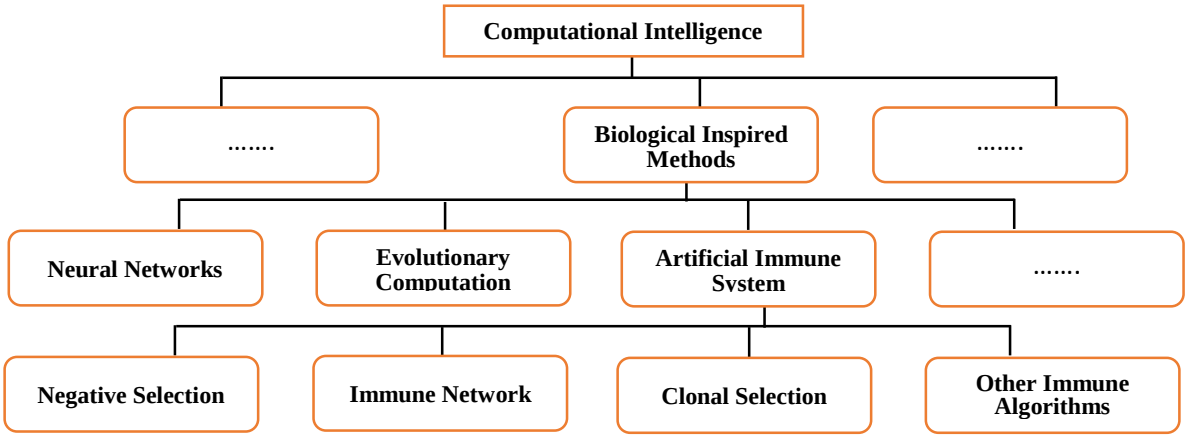


Figure 2.1. Artificial immune system as a branch of computational intelligence [39]

Artificial immune systems is a metaphorical computational intelligence system developed using ideas and theories extracted from biological immune system. It is a growing area of research attempts to bridge the disciplines of immunology, computer science and engineering, it exploits the mechanisms of the natural immune system including functions, principles and models in order to develop problem solving techniques [14, 20, 42, 43, 44]. Thus, artificial immune systems are a class of computationally intelligent systems inspired by the principles and processes of the vertebrate immune system. Computer engineers, mathematicians, philosophers and other researchers are particularly interested in the capabilities of this system, whose complexity is comparable to that of the human brain [4].

There have been a number of attempts over the years to find a commonly accepted definition for the AIS. An early attempt from Timmis [45] defined AIS as "an AIS is a computational system based upon metaphors of the natural immune system" while Dasgupta [46] defined AIS as follow: "AIS are intelligent methodologies inspired by the immune system toward real-world problem solving". De Castro and Timmis [47] then define AIS to be "AIS are adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving" [48].

Two threads of research employed jointly to accentuate the artificial immune systems field, which are mathematical and computational techniques. Although many deep investigations have been conducted to better understand the principles of human immune system but still the field not totally understood [8], later in this chapter valuable review on the evolution of the field beside close insights from AIS researchers to help make maximum benefit from AIS theory will be provided.

AIS is a very attractive computational intelligence technique, it offers a variety of paradigms that can be adapted to computational tasks [49], it is robust, decentralized and error tolerance to name a few of it is great properties providing powerful information processing and problem solving ideas [12, 50]. AIS possess great diversity of applications, techniques and models [9, 39], so algorithms and techniques have been applied to a wide range of applications such as information security, machine learning, fault diagnosis, data mining, clustering, classification, learning, image processing and robotics [34, 50, 51, 52].

Two generations of AIS can be found in literature, first generation which is relying only on simplified immune models and its algorithms have often shown considerable limitations when applied to realistic applications. It uses simplistic models of immunology as the initial inspiration, for example negative and clone selection. In contrast the second generation is

more complicated and utilizes interdisciplinary collaboration to develop a deeper understanding of the immune system and hence produce more complex models. Because of the limitations of the first generation, the second generation of AIS is emerging, using models derived from cutting-edge immunology, such as Dendritic Cell Algorithm (DCA). Both generations of algorithms have been successfully applied to variety of traditional and complex engineering problems, including anomaly detection, pattern recognition, optimization and robotics [12].

2.4 Properties of Immune System

Natural immune systems have inspired researchers to develop algorithms that exhibit its most attractive characteristics. The natural immune system is a highly distributed adaptive learning system with great properties that are widely attracted computer scientists and engineers and helped in developing and modelling solutions to different engineering problems.

Table 2.2 below shows the most interesting properties of immune system in details.

Table 2.2. Main properties of biological immune system

Property	Description
Uniqueness	Each individual has its own immune system with its own vulnerabilities and capabilities [5, 53].
Recognition of Foreigners	The harmful molecules that are not native to the body are recognized and eliminated by the immune system [5, 17, 53].
Anomaly Detection	The immune system has the ability of detecting and eliminating invaders even those which have never encountered before [5, 53, 54, 55].
Distributed (Distributability)	The immune system is a parallel system consists of diverse set of molecules distributed all over the body but still chemically interacted with no central control, this means there is no single point of failure [4, 5, 13, 17, 21, 40, 41, 48, 54, 56, 57, 58, 59].
Imperfect Detection (Noise Tolerance)	Imprecise detectors allow for generality in the matching process, an absolute recognition of the pathogens is not required, this will increase the flexibility of the system [4, 5, 13, 17, 53, 54, 55, 56, 60].
Learning	Affinity maturation guarantees that the immune system becomes increasingly better at the task of recognizing patterns. The immune network theory is another powerful example of learning in the immune system [8, 14, 40, 48, 53, 55].
Memory	Immune system learn the structure of the antigens so future reactions to the same antigens will be faster and more efficient. Some of the lymphocytes are kept as memory cells, next time the same antigen is detected, the memory cells generate a faster and intense response [5, 13, 14, 17, 59].
Multi Layered	In the immune system a multiple layers of different mechanisms are combined to provide high overall security [54]. Each layer operates independently, yet incorporates with other layers to provide a comprehensive defence-in-depth [5, 13, 40, 41, 60].

Adaptability	The immune system has the ability to continuously learn and adapt even to a changing human body environment [40, 60].
Diversity	Different people are vulnerable to different microbes [56]. A large population of cells with diverse set of receptor types enables the body to cover large portion of pathogens [4, 13, 14, 17, 41, 48, 51, 54, 55, 60].
Feature Extraction	The immune system has the ability to extract features of the antigen by filtering molecular noise from disease causing agents before being presented to other immune cells [5, 8, 14, 17, 48, 61].
Dynamic (Metadynamics)	Immune system has the ability to discard useless components and improve on existing components. Individual components are continually created, destroyed, and circulated throughout the body, this will increase the temporal and spatial diversity [17, 41, 56]. The immune system cannot maintain a set of detectors large enough to cover the whole space of all pathogens, so instead, it maintains a random sample of its detector repertoire, which circulates throughout the body. This repertoire is constantly changing through cell death and reproduction [54].
Disposability (Robustness)	No single component of the human immune system is essential, any cell can be replaced. The immune system can manage this because cell death is balanced by cell production [51, 54, 62].
Self Protecting	By protecting the body as a whole, the immune system is protecting itself, so the same mechanisms that protect the body used to protect the immune system itself. It means that there is no other additional system needed to protect the immune system [14, 56].
Autonomy (Autonomous)	The immune system does not require outside management or maintenance, each entity of the immune system operates under independent control. There is no central authority and hence no single point of failure [13, 51, 54].
Safety	The co-stimulation or a second signal and also the activation thresholds to ensure that detection errors are considered as checks-and-balances to ensure the stability of the immune system [13, 17].
Resource Optimization	Less specific lymphocytes can detect a wider variety of pathogens, this will allocate more resources since less specific lymphocytes can detect a wider variety of pathogens [54]. Also the system maintains a random sampling of the search space at any one time through the use of programmed cell death and cell division [13].
Parallel	The immune system is a massively parallel architecture with a diverse set of components. These components are distributed throughout the body and communicate through chemical signals [13, 41, 57, 59].
Lightweight	The human immune system is lightweight. This is because a vast number of antigens can be detected with a smaller number of antibodies, and the information gained from detecting antigen will be reused next time, and because limited number of antibodies will be used efficiently [58].
Self-Organization	The overall immune response and all its components are self-organizing rather than being directed by a central organ or predefined information [41, 58].
Pattern Matching (Pattern Recognition)	The immune system is able to recognize specific antigens and generate appropriate responses. This is accomplished by a pattern recognition mechanism based on chemical binding of receptors and antigens. The immune system has the ability to recognize, identify and respond to a vast number of different patterns. Additionally, it can differentiate between malfunctioning self-cells and harmful non-self-cells [4, 8, 14, 48, 61, 63].
Self-Regulation	Immune response generally uses a lot of resources to stop the attacks and eliminate its effect. Once the invader is eliminated, the immune system regulates itself in order to stop the delivery of new resources and to release the used ones and to prepare for the next one [14, 60].
No secure layer	Immune system cells are also subject to be attacked by pathogens, so lymphocytes can protect the body against other compromised lymphocytes. In this way, mutual protection can stand in for a secure code base [54].
Identity via Behavior	In the human immune system, identity is verified through the presentation of peptides, or protein fragments. Because proteins can be thought of as “the running code” of the body, peptides serve as indicators of behaviour [54].
Other attributes of immune system	Self-monitoring [60], self-learning [59], no trusted components [54], turnover of components [51].

2.5 Review of AIS Research

As addressed above, artificial immune system is offering great diversity of problem solving algorithms and techniques, it is one of the very attracting fields, which notably success in convincing researchers to start investigating and developing real-world models to non-linear engineering problems.

Two directions of research employed jointly to accentuate the AIS field, which are mathematical and computational techniques. Although many deep investigations have been conducted to better understand the principles of human immune system but still the field not totally understood [8].

When reviewing AIS literature, it has been noted to have a number of conceptual frameworks used frequently in building AIS models for different engineering applications. In the rest of this section a detailed literature review of the AIS research generally with close focus on the most important researches are provided.

Looking closely to the AIS theory after decades of research and hundreds of papers and conferences - and not ignoring those great conceptual frameworks, ideas and theories in literature – there are a real question raised on the importunateness and effectiveness of this technique. It may be the right time to take an insight look and assess AIS research contributions generally and to find new ideas allowing this field to go forward and be fully exploited since there are not many instances of AIS applications applied to real world problems or being used in industry.

Hart and Timmis [17] categorize AIS application engineering into three classes: anomaly detection, optimization and classification. Considering key works and the progress of AIS in last decade, it is important to assess the contributions of this important field into application areas to which it has been applied. Hart and Timmis argue that AIS should contain features and properties that are not present in other paradigms in order to be

considered a successful and useful field. As a way forward they proposed three suggestions for the researchers to get most benefit from AIS, which are:

1- Focus on innate immune system and cooperative solutions between both innate and adaptive immune systems;
2- Consider combining AIS with other intelligent systems to overcome individual limitations;
3- Develop more models on one of the AIS important features, i.e. life-long learning feature.

Although AIS techniques have great success in modelling solutions to real-world problems, Dasgupta [39] argued that still there are some open issues, he mentioned uniqueness and usability of each model needs to be determined as the most important issues. Dasgupta mentioned some aspects to be addressed in order to make the AIS a real-world problem solving technique [39]:

- Needed some improvement in the AIS algorithms efficiency;
- Enhancement of the representation;
- Researchers on AIS should start introducing new other immune mechanisms;
- Developing a unified architecture for AIS modelling.

Twycross and Aickelin [64] argued that AIS need to be built based on much more biologically-realistic models, and instead of building AISs based on the complex human adaptive immune system, AISs should draw inspiration from relatively simpler organisms which possess only innate immune systems, even if the built AIS incorporated adaptive immune system it should combine innate mechanisms as well since there is no organism with only an adaptive immune system. Also they emphasized the need of AIS research to be based around more sophisticated systemic models of the immune system than those currently employed [64].

Timmis et al. in [43] sees AIS as one of the genuine interaction between immunology, mathematics and engineering so the field of AIS can easily be driven a true interdisciplinary biological inspiration mechanism. According to Timmis and the team in [43] there is more attention from researchers to inspire ideas from biological immune system, so AIS is becoming a more interdisciplinary topic where two groups of researchers are present, some are focusing on biological aspects and others on the engineering aspects. The research text in [43] is concurred with a number of researches, Forrest and Beauchemin [65], Andrews and Timmis [66], Stepney et al. [32], Bersini [67], Timmis [68] and Cohen [69] concluding that engaging AIS engineers with the immunological modelling scientists are very useful for both communities [43].

Forrest and Beauchemin [65] present a conceptual paper reviewing agent based models (ABM) techniques as they applied to immunology, and argued that there is still a question about the usefulness of using agent based AIS models in understanding the natural immune system. The research paper [65] proposed a comprehensive framework for agent based models, this framework then used to create specialized models for particular applications.

De Castro & Timmis [47] proposed a generic layered approach of immune system inspired engineering solutions. As shown in Figure 2.2, this framework identifies the components that need to be address in designing and deploying AIS solution, which are: representations, affinity measures and immune algorithms.

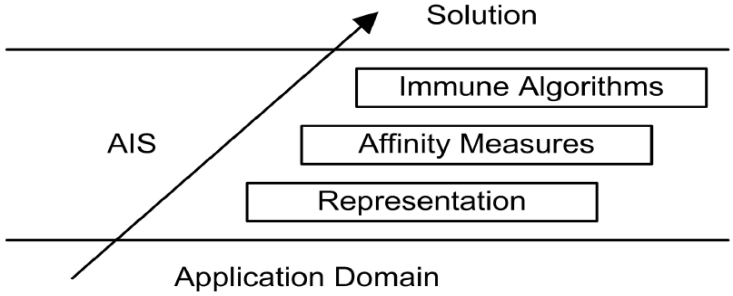


Figure 2.2. AIS layered framework - de Castro and Timmis [47]

This layered framework demonstrates the general structure of most AIS and being used frequently to describe the main AIS types. The layered framework takes the application domain of the AIS as its starting point, followed by three layers to be considered before the required AIS is engineered. These layers are: component representations which shows how the components of the system to be represented, affinity measures shows how the interactions between the components of the system are measured and quantified, and then immune algorithms which shows how the components of the systems are going to interact.

Twycross and Aickelin [1] proposed a conceptual framework for AIS incorporating properties and key roles of innate immune system, this will provide a forward step in developing more integrated AIS models.

De Castro and Timmis [9] proposed a conceptual structure for modelling and engineering AIS, with the general basis of representing and modelling immune cells and organs.

Elhag et. al. [32] also proposed a set of general-purpose algorithms to govern the dynamics of the AIS.

Wang et. al. [20] proposed a new complex AIS, in which complex representation is used as extension of binary representation and incorporated complex representation into AIS. The proposal also showed that the binary values cannot alone describe pattern recognition problems in real-life problems [20].

Tarakanov and Dasgupta [38] present a mathematical model based on the antigen–antibody bindings which is one of the great features of the immune system as a highly distributed adaptive learning system. The protein binding is represented as a mathematical abstraction for key biophysical mechanisms of proteins' behaviour. Research showed that even simple variants of immune system networks incorporates main properties of immune response [38].

Andrews and Timmis [66] considered that the majority of AIS models are based on two theories which are Burnet clonal selection theory [70] and Jerne immune network theory [71]. By investigating the state of current thinking among immunologists today, Andrews and Timmis [66] found that certain immune system concepts, such as self and non-self discrimination, are not agreed upon among all researchers. In their research paper, it is identified that possible inspiration ideas for AIS can be gained from immune system models especially new models. More theoretical understanding is required since work to date in the realm of AIS has mainly concentrated on what other paradigms do, such as simple optimization and learning. Therefore, attention should not only be paid to the potential of the immune system as inspiration, but also other systems with which the immune system interacts, in particular the immune, neural and endocrine systems. This will pave the way for a greater understanding of the role and function of the immune system and develop a new breed of immune inspired algorithms [66, 72].

Mishra and Bhusry [23] presented a research paper which reviewed major works in the area of AIS. It has been observed that most of AIS research focused on only three algorithms, i.e. clonal selection algorithms, negative selection algorithm and artificial immune networks. So writers encouraged computer scientists and engineers to evolve new models and algorithms.

Stepney et al. [32] argued that the next biological inspired computational intelligence systems should develop more sophisticated biological models. Writers also argued that these bio-inspired algorithms are best developed in multidisciplinary conceptual framework as a sophisticated biological models. In this important document Stepney et al. presented a conceptual framework in which biologically-inspired models and algorithms can be developed and analysed, this unique framework is shown in Figure 2.3 below [1, 32].

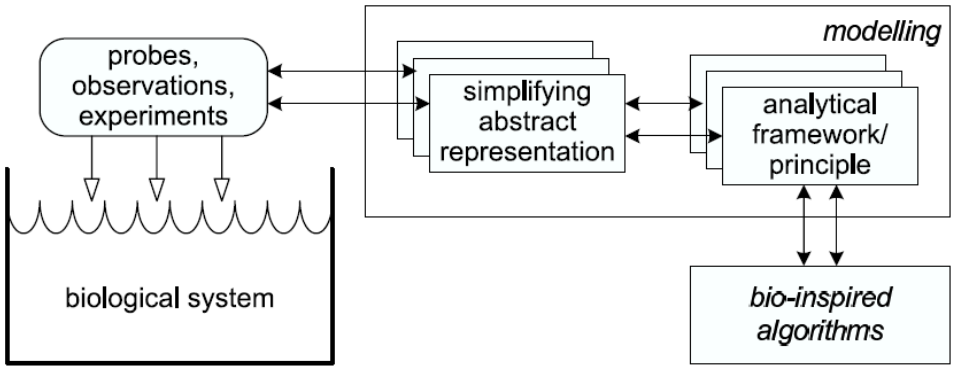


Figure 2.3. Conceptual biological inspired framework by Stepney et al [32]

Irun Cohen [69] introduced the concept of computational strategy which immune system uses to carry out its functions in protecting human body. Author invites immunologists to enlist computational scientists to help engineers and practitioners to organize, study and manipulate the enormous amounts of data have obtained by experimenting immune system. Further, the writer thought that immune computation should influence the technologies used by immunologists in modelling immune system [69].

Forrest and Beauchemin [73] provided a comprehensive review on modelling approaches in immune inspired systems and highlighted different ways of modelling immune system. Within this conceptual paper, the authors focused on agent based modelling where cells might be represented as individual distributed agents. Authors argued that Agent Based Models (ABM) might be more appropriate tool for modelling immunology due to the ease of incorporating knowledge into the model that might not be easily expressed mathematically [43].

Cohen model [74] is considered as one of the substantial models of the immune system. It presents immune system as complex, reactive and adaptive system whose role is to maintain stability to human body, this is not concur with the classical view that sees the main functions of immune system as defence mechanism against pathogen and self–non-self discrimination system. Cohen's immune theory was able to highlight a

number of ideas for inspiration that are not presented in the main algorithms of immune system like clonal selection and immune network algorithm [66].

Timmis et al. in [75] agreed with Mishra and Bhusry [23], on that many research papers that AIS technique are much more than engineering systems inspired by the immune system and they suggested that there is a great chance for both immunology and engineering to learn from each other and start working together in an interdisciplinary manner. They also argued that AIS is becoming a more interdisciplinary topic where people are working more on the biological aspects and others on the engineering aspects. So more time need to be spend to develop abstract computational models of the immune system and work closer with immunologists to better understand the biology behind the system.

Greensmith et al. [12] argued that there is a massive change in AIS research, the change is the obvious move to second-approach of AIS followed by theoretical studies of AIS and computational immunology. The change in focus of the field suggests that, as the characterization of the second-generation approaches improves, they will increase in popularity and may eventually dominate the field. Like any new discipline, the future of AIS research are not so clear, given that AIS algorithms are still evolving. As the knowledge of immunology increases among researchers and engineers, at some point in the future may have the grounding and computational resources to build full biologically accurate computational immune systems based on both the innate and adaptive systems and their numerous cell types [12].

Dasgupta and the team in their comprehensive review [44] suggested that recently the immune system has drawn significant attention to as a potential source of inspiration for novel approaches to solve complex computational problems and its great features offer rich metaphors for its artificial counterpart. For the AIS to gain more attention and to become

more valuable in problem solving, and unlike other engineering systems, AISs require both immunology and engineering to learn from each other through working in an interdisciplinary manner. A collaborative effort of several interdisciplinary research scientists has produced a prolific amount of immune inspired algorithms by extracting or gleaning useful mechanisms from the immune system theories, processes and elements [44].

According to Zhang and Yunfang [72], AIS algorithms have mainly been developed in an ad-hoc manner, with particular applications in mind. This may question the usefulness and may mean that theoretical justification for the use of AIS has mostly been lacking. The theoretical work done so far merely constitutes the first steps towards developing a more rigorous underpinning to the area, and therefore it is clearly that more remaining work is to be done. Writers seen that much work on AIS has concentrated only on simple extraction of metaphors and direct application. Despite the creation of a framework for developing AIS, it still lacks significant formal and theoretical underpinning. AIS have been applied to a wide variety of problem domains, but a significant effort is still required to understand the nature of AIS and where they are best applied.

Freitas and Timmis [76] outline the need to consider carefully the application domain when developing AIS. They review the role AIS have played in the development of a number of machine learning tasks including classification and optimization. However, they clearly pointed out that there is a lack of appreciation for possible inductive bias within algorithms and positional bias within the choice of representation and affinity measures [72].

Looking closely to the comprehensive revisions of Timmis and his team in [68] and [48], they concluded that AIS is lacking thought regarding the application areas of AIS, lacking theoretical work and limited view of immune system, and also lacking the proposal and development of a

general framework to design AIS. Comparing to other computational intelligence or soft computing paradigms, such as artificial neural networks, evolutionary computation and fuzzy systems, it is clear that there is presence of well described set of components and/or mechanisms with which to design such algorithms. He then proposed a framework which need more work in terms of formalization from a mathematical viewpoint and augmentation in terms of new shapes spaces and development of new algorithms [48, 72].

Recent researches on AIS development are also seeing AIS as a very promising and effective study area with obvious limitations and very big room of improvement. Several review papers have discussed the slow advances in AIS and proposed improvement strategies through novel and simpler AIS models, as well as the importance of developing a unified architecture for integration of existing models.

According to [77], several reviews have discussed advances in the field of AIS on a qualitative perspective. In this work, Haider et al investigated main questions about AIS research from a quantitative perspective, results shown that the field has been growing ever since it was established for the past couple of decades. Writers encouraged external scientists not only engineers to entertain the challenges presented by AIS, but also to be a benchmark for scientific domain analyses.

Mishwa et al in their research in [78] proved that the hybrid techniques used are more effective than their parent techniques, and arguing that AIS for detection research area could see a massive growth through the support of additional immune aspects such as gene libraries and idiotypic networks. Generally writers concluded that the research on the HIS is not comprehensive and there will be many more theories needed, they are certain that the performance and capability of network IDS design based on this understanding will improve.

Karin, Fister JR and Fister are encouraging AIS researchers to further extract inspiration from the components and processes from the immune system for creating effective and powerful computational systems. They are also considering that the possibilities of extracting useful metaphors and constructing new AIS theories are wide-open. They insisted that, a significant number of concepts could be used in the development of AIS in the near future, some of those concepts are clonal expansion, affinity maturation, cross-reactivity, epitope, idiotope, paratope, B-cell and BCR, T-cell and TCR, network structure, dynamics and meta-dynamics [79].

Mishrad and Husry [23] in their survey paper which highlighted the recent applications of AIS, are agreeing that AIS models have accomplished tremendous achievements in many application areas, but there are still many theoretical problems exist, and they are proposing the following solutions:

- The work should focus on expansion and advancement of the algorithms not only on the applications as been noticed now;
- Further analysed such as convergence and advancement of unified framework is needed;
- Consider combining different techniques of soft computing that includes neural network, genetic algorithm, and fuzzy logics;
- More study requires for resolving complicated real world situations and applying them to more challenging application areas like classification and future prediction problems.

According to Hang and the team [80], AIS research recently has drifted away from more biologically appealing models to biological details, such as DCA. They argued that there are powerful algorithms that have already arisen and can arise when more than two of the different approaches are hybridized or new HIS theory is proposed.

2.6 Applications of AIS

AIS is a steadily progressing branch of computational intelligence field and is considered one of the very attractive fields with great diversity of applications. Those applications are well addressed in tens of research papers in developing solutions to complex non-traditional problems. As illustrated in Figure 2.4, the AIS applications can generally be categorized into three categories as follow [8, 17]:

1. Anomaly detection
2. Optimization
3. Learning (or clustering and classification)

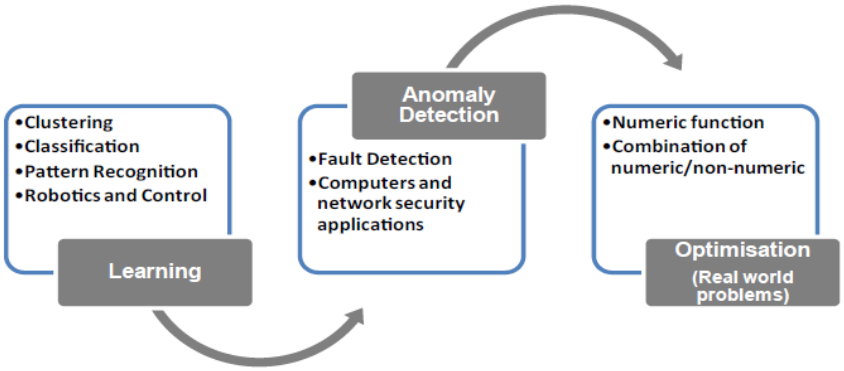


Figure 2.4. Applications of AIS [8, 17]

Looking closely to the AIS literature, it can be observed that AIS have been applied to a wide range of application domains, this was started from the early 1990s when immune system metaphors was undertaken in the area of fault diagnosis [81] then later applied to field of computer security and virus detection [82] and that was just the start.

Table 2.3 below shows detailed information on the main applications of the artificial immune system found intensively in literature.

Table 2.3. Applications of AIS with research examples

Application Area	Description	Examples
Network Security	The role of the immune system to protect human body from invaders is analogous to that of computer security systems specially IDS/IPS.	[19, 39, 53, 83, 84, 85]
Anomaly Detection	The problem of detecting anomalies can be viewed as finding deviations of a characteristic property from the normal profile [86].	[14, 53, 87, 88, 89, 90]

Data Mining	Also called knowledge discovery in databases, is related to the process of identifying and extracting valid and potential patterns or knowledge in data [86].	[28, 91]
Pattern Recognition	Is the research area that studies the operation and design of systems that recognize patterns from data, systems like discriminant analysis, feature extraction, error estimation, cluster analysis, etc. are considered sub-discipline of pattern recognition [86].	[92]
Adaptive Control	Is the capability of the system to modify its own operation to achieve the best possible mode of operation.	[53, 93]
Optimization	"Optimization is the task of finding the absolutely best set of admissible conditions to achieve a certain objective, formulated in mathematical terms" [86].	[94, 95, 96]
Fault Detection	The type of control system concerns with monitoring a system, identifying when a fault has occurred, and pinpointing the type of fault and its location.	[97, 98]
Clustering	Clustering is a machine learning technique that involves the grouping of data points that are similar in some way.	[27, 51, 99, 100, 101]
Classification	The main role of immune system according to most of the researchers is to classify between self and non-self cells. So classification is the most wide used application domain of AIS [102].	[31, 49, 103, 104]
Learning	Learning is usually addressed to the processes of acquiring knowledge from experience and abstracting this knowledge to solve new, previously unseen problems. The process of immunizing (through vaccination, for example) is a clear example of an immune learning mechanism. Similar strategies can be used to solve problems like pattern recognition, concept learning, etc.	[11]
Machine Learning	Several machine-learning strategies are being used to solve problems like function approximation and optimization. Machine learning is focussing on finding patterns from asset of data coming from a source of interest. Feature based and similarity based approaches are two main machine learning techniques [51].	[51, 105]
Robotics and Autonomous System	Robots is a programmable manipulators designed to move and perform tasks. One of Robot most difficult tasks is the Autonomous Navigation problem, where a robot has to perform certain tasks without any external guidance.	[26, 99, 106]

2.7 Similarities between HIS and Computer/Network Security or IDS

Through decades of biological inspired systems research, it is realized the high similarity between human immune system and the computer and/or network protection systems specially Intrusion Detection System (IDS). This remarkable similarities led to thousands research papers and books on the use of the artificial immune system theory in security generally, and IDS application in particular [7, 34, 54, 89, 107].

The main function and objective of the human immune system is to protect human body from malicious invaders by discriminating between self and

non-self molecules, like the human immune system, computer and network security systems, especially IDS, are also to defend the network or computer systems from malicious attacks and unauthorized intruders [7, 21, 56, 108].

There are many similarities between human immune system and intrusion detection system can easily be noticed, such as:

- The task of both are the same; The IDS task is to detect attacks and to take suitable defensive reaction without reacting to the normal behaviour. In the other hand the main task of the human immune system is to distinguish between self and non-self cells and to eliminate antigen cells without reacting to self-cells [84];
- An intrusion detection system like HIS is expected to evolve and improve over time to be able to combat new type of attacks [34];
- The environment of both IDS and HIS are quite similar. The environment where computer systems and networks are functioning these days is complex and changing specially when connected to internet considering a wide range of viruses and intrusions and all different kinds of threats and vulnerabilities. An HIS is also existed in a complex and changing environment with thousand types of diseases and pathogens [84];
- HIS and IDS are both intended to analyse and deal with a large amount of data [34];
- Both have to maintain stability in a very dynamic and changing environment [109];
- Both systems are using misuse and/or anomaly detection mechanisms [84, 110].

It is also noticed that there are great similarities in behaviour between malicious software and their biological counterpart. Trojan horses get into computer network and acting as a legitimate program then turns into

malicious application inside the network. Worms self-replicated and affected the protection system and create backdoors for the entrance of more dangerous attacks. Rootkits help malware to remain hidden. A Botnet acts in a high distributed system with a well synchronized performance in order to achieve a massive attack [63].

The analogy between protecting human body and protecting computer systems or networks is evident. Computer viruses, IDSs, securing wireless networks, LAN security and many other security related researches using immunity inspired ideas can be found in massive volume in literature [56, 63].

Researchers have map in most cases the AIS with IDS or network defence systems in relatively same way; AIS is represented likely as an IDS system and self-cells are normal traffic whereas non-self cells are abnormal or attacks.

Zheng and the team [84] proposes a multilayer networks intrusion detection system combining the general characteristics of innate and adaptive immune systems. Table 2.4 shows mapping between biological immune system and network intrusion detection system as proposed in [84].

Table 2.4. Mapping between AIS and IDS by Zheng et al. [84]

Biological Immune System	Network Intrusion Detection System
Self antigens	Normal programs, network behavior
Non-self antigens	Malicious programs, network attacks
Artificial T-Cells	T-Cells detectors
Immature antibodies	Immature detectors
Mature antibodies	Mature detectors
Memory antibodies	Memory detectors
Antigen presenting cells	APC detectors
Cell clonal expansion	Mature detectors replication
Self tolerance process	Negative selection process
Co-stimulation message	Activation of negative selection
Antigens immune response	Recognition normally by detectors

Qing Hua et al. [7] proposed an intrusion detection system based on artificial immune system theory, the system used TCP/IP connection

attributes like IP address, source and destination ports, time stamp, etc. to define the normal and abnormal sets. The self and non self defined as normal and abnormal TCP/IP connections respectively.

Chen et al. [6] proposes a new model of active defense system based on AIS theory. The active defense system is mapped with the biological immune system and the hosts are the cells of the immune system. The whole mapping relationship is shown in Table 2.5 below.

Table 2.5. Mapping active defence system with AIS by Chen et al. [6]

Biological Immune System	Active Defence System
Organism	The whole network
Organ	The network segment
Cells	Hosts
Vaccine Distribution	The distribution of intruding information
Antigen	Binary strings extracted from IP packets
B-cell, T-cell, antibody	Antibodies expressed by binary strings
Clone cells	The copy of antibody

Luther and the team [111] proposed an anomaly based IDS inspired by biological immune system, The proposed AIS is mapped with packet-based intrusion detection system and the detectors are represented by a binary string with the data path triple (IP address, protocol and port).

Gullen and Paez [63] briefly analyzed the possible use of AIS in a secure network architecture implemented with future research projects. They are suggested an easy way to map pathogens and antigens with malware and network attacks, immune cells with detectors, proteins with strings, immunological response with elimination strategies.

Based on the comparison showed in Table 2.6 below, Yousef Farhaoui proposed an intrusion detection and protection system (IDPS) framework which is designed and implemented using two immune systems theories which are clonal selection algorithm and negative selection algorithm [112].

Table 2.6. Comparing immune systems and IDPS [112]

Immune System	IDPS
Thymus and bone marrow	Primary IDPS (Supervisor)
Lymphnode	Lymphonode local host
Antibody	Detector

Antigen	Intrusion
Self	Normal activity
Non self	Abnormal activity (suspicious)

2.8 Intrusion Detection System (IDS)

An intrusion detection system (IDS) is an automated system designed for the purpose of detecting computer system intrusions from both internal and external intruders and is considered an ordinary component of network security since the 1980s, it is a type of security software designed to automatically alert administrators when it detects any abnormal activities [41, 58, 84, 107, 113, 114].

Intrusion detection is the process of intelligently monitoring the events occurring in a computer or network and analyzing them for sign of violations of the security policy, it is also intended to detect malicious activities and determine their nature, origin and seriousness. The IDS is aiming to enhance the overall security of the system and to ensure availability, confidentiality and integrity of information [84, 107, 108, 115, 116].

The need of a system with special focus on detecting attacks and misuse specially those committed from outside network is obvious, considering that traditional passive defence technologies like encryptions and firewalls are not enough to secure networks completely and cannot fully meet the required security measurements in internet environment [114, 117].

Recent developed IDSs provide an additional layer of defence beside other layers such as physical, authentication and access control. Since the perfect IDS has still not been developed yet in spite of the great research efforts, researchers are heavily considered bio-inspired algorithms in building intelligent IDSs such as Genetic Algorithm, Artificial Neural Networks and Artificial Immune Systems [110, 117].

Many challenges are facing the deployment of IDS in a complicated network environment, one of those challenges is the ability to analyse the huge number of alerts generated every day by IDS. Also the IDS have

some difficulties to adapt to the changes of the network architecture and lacking self adaptation, other well-known challenges of existing IDSs are their high false positive rate and their abilities to detect only known attacks while failing to detect new and unknown attacks [6, 33]. Intrusion detection technology also lacks robustness since local error can affect the whole system [6].

2.8.1 Placement

Network administrators are either placing intrusion detection systems on a host or on a network node, using any one of these strategies is depend on the size of the network and the level of security needed. Some network administrators applying both placement strategies, but this is not so common. In general, most of the recent IDSs are network-based while that was not the case in the past where most of them were host-based [58, 110]. Recently another category is emerging to be a new IDS category which is application-based IDS, this type is considered in most security handbooks as host-based IDS since applications are installed in a network hosts at the end of the day, also they are both sharing number of characteristics such as being able to decrypt and analyse encrypted traffic [118].

A host-based IDS (HIDS) is a computer program or software installed on a single host machine for monitoring the behaviour of a host. It analyses events and logs of running operating system and applications and send any detected intrusion or suspected behaviour to the administrator for further investigation or immediate action. Examples of HIDS are Snort, Samhain and Prelude [5, 110].

HIDSs have many advantages make them so effective in specific situations. For instance, HIDS can monitor and analyse encrypted traffic, unlike Network-based IDSs (NIDS) which have notable difficulty to deal with encrypted data. Another important advantage of using HIDSs is that it can provide detailed forensic information from monitored host. This is

due to HIDS capabilities of monitoring host specific system activities. Also HIDSs can better detect attacks occur in the host itself which are not easily detected by NIDS [118].

Network-based IDS (NIDS) is found in a specific hardware and normally used for commercial purposes. This device is installed in a single network node but can monitor any number of hosts on a network, and any traffic go through this node is captured and analysed [58, 110].

The NIDSs are easier to manage and costs less than placing a HIDS in each host or in a number of hosts. Since NIDS can be placed before firewall this can help identifying patterns of intrusions and can give forewarning information. The NIDS have more vision on the attacks behaviour unlike HIDS which is only monitoring single host, this can help NIDS catches attacks that may be missed by HIDS [118].

2.8.2 Detection Mechanism

Intrusion detection systems generally employ two different approaches to fulfil its duty to detect intrusions or attack attempts, i.e. misuse detection mechanism, also known as signature based, and anomaly detection mechanism.

Some IDSs combine techniques of misuse and anomaly detection to construct hybrid intrusion detection system with capabilities of detecting intrusions using database signature which is good for detecting known attacks and uses anomaly detection approach to detect unknown attacks as well. Also computational and/or artificial intelligence techniques are widely applied to build intrusion detection mechanism such as Fuzzy Logic/Expert System, Pattern Recognition System, Neural Networks and Artificial Immune System [115].

Most of the current available IDSs are signature based, which is the one most used in commercial products [110, 118]. This approach relies on matching predetermined signatures extracted from previous known

attacks and vulnerabilities and stored in a database with the signature of monitored traffic, this explains why signature based intrusion detection systems have the ability to detect known attacks but failed in most cases to do the same with novel attacks [58, 60, 108, 114, 119].

Many reasons can affect the efficiency of misuse detection approach such as [110, 115]:

- The availability of the attack patterns;
- Time needed to develop new attack patterns;
- No new signature yet;
- If signature database is out of date;
- If the signatures are too specifically bound to a given attack.

Anomaly detection approach on the other hand is of great interest to network security researchers but is rarely used in commercial products. This approach is showing encouraging results in reacting to new attacks with higher false positive rate than signature based IDS when reacting to known attacks. Detecting yet unknown attacks or zero-day attacks is also useful in generating a signature to be used by the misuse detection as well [60, 110].

The anomaly detection mechanism relies on detecting unusual behaviour of a network traffic like a massive CPU consumption or a big number of packets from a specific IP Address. In the anomaly detection process the normal behaviour profile should be created by training and monitoring legitimate traffic, then incoming traffic will be compared with this normal behaviour to detect any variations [58, 60, 84, 110, 117].

Anomaly detection based approach is also facing some difficulties and issues, the common one is the requirement of extensive training for the data, this problem have impact on expenses, efforts needed and quality of the output. Also, as declared earlier, the anomaly detection IDSs still having the higher rate of false alarms this could be reduced when applying hybrid IDSs which utilizing the capabilities of both approaches [115, 118].

2.9 IDS/Network Security Systems Using AIS

For decades computer and network security systems have faced a challenge of determining the difference between normal and potentially harmful activities. For half a century, developers have protected their systems using rules and signatures by comparing collected patterns with normal and abnormal patterns extracted from those rules. However, the nature of current and future threats in conjunction with ever larger and complicated IT systems urgently requires the development of automated and adaptive defensive tools. A promising solution is emerging in the form of hybrid security systems using biologically inspired computing, in particular artificial immune systems. The biological immune system can detect and defend against harmful and previously unseen invaders [120]. Inspired by the many excellent characteristics of biological immune system, more and more computer security researchers integrate biological immune mechanism into the network intrusion detection technologies, the network intrusion detection system (NIDS) which based on artificial immune system has become one of the focus of the intelligent research and achieved many good results in the recent studies [84].

Great massive researches on network security generally and IDS particularly inspired by human immune system can be found in literature. Table 2.7 below shows number of good examples of such researches.

Table 2.7. Examples of IDS and/or network security systems using AIS

Reference	Description
Hofmeyr and Forrest, (1999) [56]	Focused on protecting a local area broadcast network from attacks using artificial immune system theory and algorithms. It described in details the proposed architecture for an adaptive artificial immune system incorporating several forms of adaptation on different time scales. The paper also addressed an important problem of network intrusion detection and then showed how to embed an architecture for adaptive behaviour in a real-time network environment with live agents.
Jiandong et al., (2005) [121]	A follow work of the same writer's series of papers which intended to construct an integrated security local area network. It describes a top level architecture of artificial immune system for LAN constructed using AIS switching nodes. The research argues that implementing AIS network basing on IXP2800 will give higher performance and more protection to networks.

Dasgupta, (1999) [122]	Proposed an agent based artificial immune system for protecting local networks. The proposed system has number of unique features compared to the existing agent-based detection systems like simultaneous multi-level monitoring, detection of known and unknown intrusions, and hierarchical sense and response mechanisms beside common features such as immunity based mobile agent's role, adaptivity, self-regulation, life cycle, specificity and diversity. The proposed system can perform in real-time with capabilities of monitoring, analysing and generating appropriate response to intrusive activities.
Zhang et al., (2008) [6]	Presented an effective artificial immune system multi-hierarchy framework model for active defence network security. The proposed model inspired by immune system main features like parallel and distribution defence capabilities and thus utilizes these characteristics to provide an effective solution for the network intrusion. The experiment results show the effectiveness of this solution as an active defence system for protecting networks and single PCs.
Middlemiss and Whigham, (2006) [123]	Proposed a cooperative framework for an artificial immune system that incorporates innate and adaptive concepts capable of recognising dangerous behaviour within an intrusion detection system. The research described the importance of having both systems innate and adaptive systems acting cooperatively. It described a simplified view of the immune system and characterized some of the known properties of this system in terms of a rule and feature-based model.
Powers and J. He, (2008) [119]	Proposed a hybrid IDS inspired by artificial immune system theories, the system combines the two know IDS approaches anomaly detection and misuse detection with the aim of combining the advantages of both approaches. The main contribution of the proposed work is the use of separate components for anomaly detection and attack classification.
Twycross et al., (2010) [124]	Described and tested a complex AIS model inspired by the interactions between the innate and adaptive immune systems. The proposed model performance on a realistic process anomaly detection problem is shown to be better than using known AIS algorithms like negative selection algorithm, policy-based anomaly detection methods and an alternative innate AIS approach.
Luther et al., (2007) [111]	Presented an agent based biological immune system which simulated a cooperative intrusion detection approach, a P2P communication techniques is used to develop a distributed anomaly detection scheme and to ensure communication between AIS agents. A dynamic collaboration between individual artificial immune system (AIS) agents utilized to address one of the main issues of anomaly detection IDSs which is the false positive problem.
Gonzalez and Dasgupta, (2003) [14]	The main goal of the research is to examine and to improve the anomaly detection function of artificial immune systems, specifically the negative selection algorithm and other self/non-self recognition techniques. The research investigates different representation schemes for the negative selection and proposes new detector generation algorithms suitable for such representations.
Twycross, (2007) [89]	Proposed a problem solving intelligent system inspired by immune systems metaphor, the text also explored the design and application of artificial immune systems (AISs). The thesis argued that there are more need AISs which are based on much more biologically realistic models instead of building of AISs employing only adaptive immune system mechanism, as these are not biologically realistic since they disregard the central role of the innate immune system as recent researches see it as a controller of the adaptive immune system.

Harmer et al., (2002) [13]	Presented the design of an artificial immune system (AIS) for computer security problems, the proposed design is intended to integrate the power, flexibility, adaption, and capabilities of the BIS into an architecture realizable in the computer security system as an information system domain. An agent paradigm to simulate immune system detection and communication mechanisms used because of the performance limitations of a monolithic implementation and the biological basis for the architecture can be viewed as a system of collaborating agents.
Seredynski and Bouvry, (2007) [88]	Presented an anomaly detection system inspired by artificial immune systems theory. Then it provided deep insight to an efficiency of different methods of generation of detectors since the cost of generation of antibodies is highly affecting the cost of constructing the proposed framework.
Kim and Bentley, (1999) [58]	Provided a survey on network-based IDS's literature and provided a set of general requirements for them in order to guarantee their efficiency. It is also investigated the analysed the artificial immune system research and its inspired capabilities in detection and classification. The research proposed an IDS based artificial immune model, which actually monitors a real network.
Kim et al., (2007) [120]	Reviewed research of IDS using AIS metaphor and showed the efforts of different researchers in overcoming intrusion detection problems with focus on solutions provided by artificial immune system algorithms. It is also summarized and described the main immune features that are desirable in an effective IDS which are: distributed, multi-layered, self-organised, lightweight, diverse and disposable.
Qiang and Yiqian, (2010) [125]	Proposed a network security assessment model based on artificial immune which proved to be good solution for network security situation real time assessment. The assessment model a mathematical expressions for immune elements such as antibody and antigen were built in network security environment. The network security situation assessment model based on artificial immune abstracts and expands the immune mechanism of self body tolerance, immune memory and immune monitor etc.
Kim Bentley, (1999) [126]	Investigated the existing network-based IDS's and categorised them into three approaches: monolithic, hierarchical and cooperative. The research proposed a novel artificial immune model composed of three evolutionary stages: gene library evolution, negative selection and clonal selection which are then combined into a single methodology. The model aim is to design an effective IDS with three main requirements: being distributed, self-organising and lightweight.
Sadeghi, Zahra and Bahrami, (2013) [127]	Proposed an anomaly detection system based on negative selection for the purpose of increasing the speed of intrusions detection. The proposed model intended to increase the speed of the intrusion detection by clustering and reducing the number of detector sets. The experiments using KDD Cup dataset show improvement in the speed of detection almost by 50.45%.
Zhang et al, (2008) [7]	Provided a detailed review research on immunity-based technical research of network intrusion detection. The research reviewed the IDS development technology and then discussed those IDS research models based on artificial immune system theories and algorithms.
Rui and Wanbo, (2010) [109]	Proposed an immune-based intrusion response model inspired by immune system features like self-learning and diversity. The proposed system is provided acceptable results in recognizing unknown attacks and classify them. In proposed model a dynamic response decision making mechanism is well established, which can dynamically adjust the defending strategies according to the changing environment and use the minimum cost to guarantee the safe of a system.
Singh et al., (2013) [128]	A hybrid artificial immune model for IDS simulation has been proposed in which intrusion detection takes place using Dendritic Cell Algorithm and Dempester belief theory along with SVM classification algorithms.

	Experiments showed that the proposed architecture improve the efficiency of the intrusion detection system.
Yang et al., (2011) [83]	A new network security evaluation method using antibody concentration to quantitatively analyse the degree of intrusion danger level is presented. The research proposed a multi agent framework for network security evaluation. Experimental results show great enhancement in detection efficiency and assures steady performance in the ability of intrusion detection.
Shen et al., (2012) [129]	Presented an improved AIS based intrusion detection system with both capabilities: anomaly detection and signature based. The proposed algorithm uses Rough Set feature selection algorithm for reducing complexity. The anomaly detection in the system is set up using negative selection algorithm which is used to match invaders with detectors without reacting to the own cells of the body.
Zhang et al., (2011) [130]	Proposed a smart grid distributed intrusion detection system which is a multi-layered, distributed system with three defensive layers of communication network. The proposed system is capable of analysing communications traffic using an analysing module (AM) that leverages artificial immune system module for detecting attacks and analysing them.
Zhang et al., (2013) [84]	Proposed a novel multi-layered immune network intrusion detection model, the architecture proposed is a cooperative system between innate and adaptive immune mechanisms based on pattern recognition receptor (PRR) theory. Analysis and experiments show that the model is effectively integrates the misuse detection and anomaly detection technologies to quickly respond to known network intrusion attacks and discover unknown network intrusion attacks as well.
Shen and Wang, (2011) [117]	Poposed an artificial immune system based intrusion detection system with some efficient feature selection algorithms. Negative selection algorithm is used for anomaly detection in the system. Different feature selection algorithms compared and tested using KDD cup dataset and an optimized feature selection and parameter quantization algorithms are defined. Experiments proved the outstanding detection accuracy of the system.
Tedesco et al., (2006) [131]	Presented a novel intrusion detection algorithm based on the artificial immune system integration between innate and adaptive layers drawing on theoretical models of innate immunity. The goal of the system is to discover packets containing novel variations of attacks covered by an existing signature base. The basic approach is to apply AIS techniques to detect packets which contain variations of attacks with the aim of integrating AIS components with existing intrusion detection and alert correlation systems in order to gain additional detection capability.
Hofmeyr and Forrest, (2000) [132]	Proposed lightweight intrusion detection systems based on AIS incorporating many properties of natural immune systems, like diversity, distributed, error tolerance, learning, adaptation and self-monitoring. The proposed general framework is a distributed adaptive system and could be applied to many domains.
Abas et al., (2015) [133]	Proposed a network intrusion detection system based on artificial immune system, it used Gure Kddcup data set with less features for reducing complexity and improving detection accuracy. Also an optimized feature selection of rough set theory used for enhancing time consuming.
Aickelin et al., (2003) [134]	Presented an intrusion detection system based artificial immune system with the aim of replacing the classical self-nonself viewpoint in AIS based IDS with the danger theory. In this relatively emerging theory the natural immune system does not rely on self-nonself discrimination but identifies danger.

Chan et al., (2013) [135]	Proposed an intrusion detection system based on clonal selection approach of the artificial immune system as well as negative selection algorithm which is applied alongside clonal selection classifier. A clonal selection classification algorithm has been successfully implemented to classify self and non-self-sets. The proposed study provided a review on network intrusion detection anomaly based approach.
Rihab Khairi (2015) [62]	The aim of the study is to apply artificial immune system with Real-Valued Negative Selection Algorithms for anomaly detection problem through classification of four datasets.
Igbe et al., (2016) [136]	Provided a network intrusion detection system using adaptive immune system framework through unsupervised machine learning methods. Genetic algorithm was explored as a technique for generating the detectors which form the building block of the negative se lection algorithm. Also, the performance of other techniques including J48, SVM and Naïve Bayes were compared to the proposed algorithm.
Igbe (2019) [21]	A human immune system based anomaly detection techniques for detecting cyber-attacks is presented in an attempt to solve the issues associated with anomaly-based detection systems. Two HIS models is investigated, the HIS theory of self-nonself (SNS) and the danger theory (DT).
Obinna and Saadawi (2018) [137]	Presented an anomaly detection system for detecting insider threat activities in an organization using negative selection algorithm. The proposed system classifies a selected user activities. Results show that the proposed method is very effective in detecting insider threats.
Guillén and Páez (2010) [63]	Analysed the possible use of AIS to provide an interactive security scheme, not only at the final equipment but also in a Bio-inspired complete network defence architecture.
Ortuño et al., (2016) [138]	Discussed intrusion detection systems based on computer networks and a model for the detection of malware using artificial immune system (AIS). The proposal used the ClonalG algorithm which provides good preliminary results.
Saurabh and Verma (2018) [139]	Presented an agent based artificial immune system (IICASS) which build appropriate profile of self and non-self by using limited information. Fine tuning and voting powers IICASS to have self-learning and adaptive capabilities that reflect in high detection rate with low false alarm rate for new and unseen intrusions. Collaboration and communication between agents make IICASS distributed, robust, autonomous, adaptive and self-configuring with self-learning capabilities.
Yousef Farhaoui (2017) [112]	Proposed a framework for intrusion and protection system inspired by natural immune system and implemented by using a directed approach. The study focused on the two main theories that are the basis of the immune response, namely the theory of clonal selection and the theory of negative selection. The study of these two immune theories, in the case of intrusion detection, shows that the theory of clonal selection is more appropriate for the scenario analysis, while the theory of negative selection is more appropriate for behavioural analysis.
Nguyen1 et al., (2018) [140]	Introduced a deep learning based bio-inspired algorithms that achieves a detection rate of 98.8% over an experimental dataset of total around 9300 software binaries. The research indicates that the new approach using the combination of deep learning and artificial immune system opens a new prospect for dealing with the virus detection problem.
Hosseinpour et al. (2014) [60]	Presentd an intrusion detection system architecture based on the artificial immune system concept. The proposed framework is a multilayer system since both innate and adaptive layers are presented. An innate immune mechanism through unsupervised machine learning methods is proposed to primarily categorize network traffic to “self” and “non-self” as normal and suspicious profiles respectively. The adaptive immune system in the

	proposed architecture also takes advantage of the distributed structure, which has shown better self-improvement rate compare to centralized mode and provides primary and secondary immune response for unknown anomalies and zero-day attacks.
Mahajan and Suryawanshi (2017) [141]	Proposed a two levels IDS, the proposed work aims to improve the efficiency of the current AIS based IDS systems. The project aims also to build efficient algorithms those will overcome the limitations of current systems.
Dutt et al. (2016) [142]	Proposed a two layers of defenses capability, innate and adaptive which are implemented to mimics the natural innate and adaptive immune systems. The adaptive layer incorporates T-cell and B-cell defensive mechanisms. The results exhibit that the proposed methodology works efficiently for detecting intrusions.
Behzad, Shahram, et al. (2020) [143]	Proposed a new approach, to improve the security of DSR routing protocol to encounter the black hole attacks. This schema tries to identify malicious nodes according to nodes' behaviors in a MANETs and isolate them from routing. The AIS-DSR is evaluated through extensive simulations in the ns-2 environment. The results show that AIS-DSR outperforms other existing solutions in terms of throughput, end-to-end delay, packets loss ratio and packets drop ratio.

2.10 Fuzzy Logic System for AIS

Fuzzy logic system was first introduced by Lutfi Zadeh in 1965, which can be described as a multi-valued logical representation and modelling of systems with imprecise and incomplete information. Fuzzy logic allows approximate values and inferences under uncertain conditions and deals with degrees of membership and can model and control systems with nonlinearity [3, 144].

Fuzzy logic incorporates human knowledge and experiences and deals with human reasoning on a higher linguistic, so logical notions such as ”very high” can be formulated and applied in a more human-like way of thinking. Fuzzy logic is able to process incomplete data and provide approximate solutions to problems other methods find difficult to solve. It converts human supplied rules to mathematically equivalent formulations which can easily be designed and implemented, this will accurately represent the simulated system [3, 144, 145].

Fuzzy inference is the actual process of mapping from a given input to an output using fuzzy logic and explains the actual steps involved in creating a fuzzy logic system. There four steps of fuzzy reasoning:

1. Compare the input variables with the membership functions to obtain the membership values of each linguistic label (fuzzification);
2. Combine the membership values on the premise part to get degree of membership (or strength) of each rule;
3. Generate the qualified consequents (either fuzzy or crisp) for each rule;
4. Aggregate the qualified consequents to produce a crisp output (defuzzification).

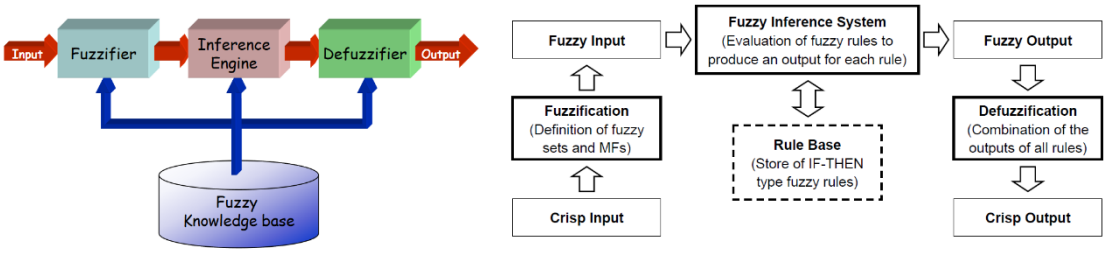


Figure 2.5. Components of the fuzzy logic system

There are four main components of fuzzy logic system as illustrated in Figure 2.5, which are:

- Fuzzy Knowledge Base: The rule base or the knowledge base is the database containing a number of fuzzy IF–THEN rules which defines the membership functions of the fuzzy sets used in the fuzzy rules;
- Fuzzification: converts the crisp input to a linguistic variable using the membership functions stored in the fuzzy knowledge base. So here fuzzy sets defined and the degree of membership of crisp inputs in theses fuzzy sets defined too;
- Inference Engine: evaluate If-Then type fuzzy rules to produce fuzzy output for each rule;
- Defuzzification: converts the fuzzy output of the inference engine to crisp using membership functions analogous to the ones used in the fuzzification.

Researchers have used the concept of fuzzy logic together with the artificial immune system and other computational intelligence systems in designing and modelling solutions to complex real problems. The examples noticed in the literature were so encouraging when applying fuzzy logic in security application generally and in intrusion detection particularly. For instance, Piyakul Tillapart and a team [146] propose a framework for intrusion detection system over TCP/IP network and use fuzzy rule-base in detecting intrusions.

Mu-Chun Su et al. [11] presents an on-line learning neuro-fuzzy classification system inspired by immune systems metaphor. Mehdi Bateni et al. [33] presented an automated alert correlation approach using both fuzzy logic and artificial immune system. In [35], Shahaboddin and the team introduced a bio-inspired system which utilizes both fuzzy and artificial immune system for detecting intrusion in wireless sensor networks.

Bridges et al. [147] proposed a prototype intelligent intrusion detection system, the system developed to demonstrate the effectiveness of fuzzy logic and neural immune system in intrusion detection application. Shanmugavadivu and Nagarajan [148] proposed a fuzzy logic based intrusion detection capability with effective automated strategy in generating fuzzy rules. In [149], Dhanalakshmi and Ramesh presented an intrusion detection system that integrates fuzzy logic and data mining along with genetic algorithm. Nasaroui et al. [25] proposed a fuzzy AIS model, which uses fuzzy set to model the area of influence of each B-cell, this will make it more robust to noise.

Lin et al. [150] presented an intrusion detection model based on fuzzy logic system theory using a new rule mining algorithm based on fuzzy sets. Norbik Bashah et al. [115] proposed an intelligent hybrid intrusion detection system which combines anomaly and signature based

approaches, the proposed system based on fuzzy logic and neural network together.

Xian et al. [27] presented a novel unsupervised fuzzy clustering method based on clonal selection algorithm for anomaly detection. Experimental results show that this method can detect unknown intrusions with higher positive detection rate.

CHAPTER THREE

HUMAN IMMUNE SYSTEM

3. Human Immune System

3.1 Overview

This chapter describes in details the biological immune system characteristics and main functions, it provides high level information on its structure, anatomy and protection strategies which has been inspired solutions to network and computer security problems.

The chapter introduced immune system layers of defence with close focus on adaptive and innate layers. Both layers are described showing the different ways of detecting and eliminating pathogens. The chapter also introduced the innate immune system central role on human immunity which was not clearly addressed in many of the researches and systems designed from the ideas and inspiration of the immune system metaphor. Then it addressed the interactions and integration among different components of the system mainly adaptive and innate subsystems and how different immune cells collaborate to guarantee stability of the whole system.

Last, the main algorithms of the human immune system were presented with a detailed literature review for each.

3.2 Structure of the Biological Immune System

The natural immune system is a complex network of great variety of specialized cells, molecules and organs spread all over the body in the search for malfunctioning cells from our own cells (infectious self) or foreign disease causing microorganisms (infectious nonself) then it responds by eliminate those infectious agents or neutralize them [5, 14, 22, 42, 89].

Although the exact function of the biological immune system is still a source of continuous debate, it is commonly agreed that the immune system main role is to protect human body from microorganisms and viruses that are capable of causing illness, those invading organisms are

called pathogens [14, 22, 108, 151]. It is an adaptive system that has evolved to provide protection against pathogens through sophisticated pattern recognition and response mechanisms and depending on the type of invaders, the damage it can cause and the way it enters the body [152]. To be so effective immune system must distinguish between self and non-self molecules, the self/non-self discrimination capability is considered as one of the important characteristics of the immune system [14, 42, 153].

Immune System is highly complicated system possess powerful information processing capabilities it is adaptive learning, parallel, highly distributive, multi-level protective system with no central control, these unique characteristics and others caught the attention of scientists and researchers for decades [42, 108, 122].

Immune System has excellent ability to recognize the foreign molecules, even when they are not seen before, the memory characteristic of immune system allows it to identify invaders when encountered human body again [8, 60].

3.2.1 Anatomy of the Immune System

Immune system is an adaptive distributed system composing of millions of white blood cells spread all over the body known as lymphoid organs.

The lymphoid organs are divided into two main types, primary lymphoid organs where immune system cells are produced and mature example of this type are thymus or bone marrow, and secondary or peripheral lymphoid organs where those cells compared with other cells looking for antigen; examples are spleen or lymph nodes [5, 89].

Figure 3.1 shows the lymphoid organs, how and where exactly they are spread all over the human body and Table 3.1 describes their main functions.

Table 3.1. Lymphoid organs and their functions

Lymphoid Organs	Function
Tonsils and Adenoids	Contains immune cells mainly protect the respiratory system

Lymphatic Vessels	Assist lymphatic cells and antigens to move to the immune organs and blood
Bone Marrow	Site where immune cells are produced
Lymph Nodes	Sites where immune cells are stored
Thymus	Site where cells are mature and multiply if necessary
Spleen	Site where the leukocytes destroy or neutralize invaders of the blood stream
Appendix and Peyer's Patches	Contains immune cells mainly for protecting the digestive system

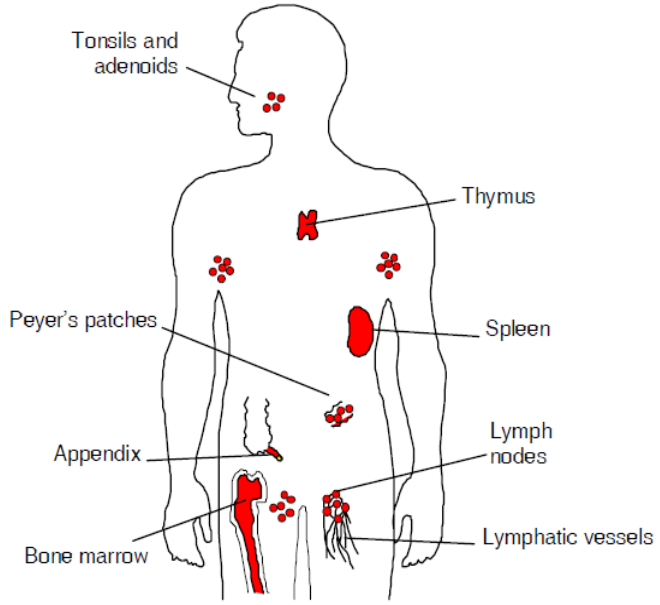


Figure 3.1. Distribution of the lymphoid organs in human body [5]

As illustrated in Figure 3.2 the biological immune system provides a multilayer form of defence capabilities where each layer employs different types of defence mechanisms for detection, recognition and responses to harmful stimulus [39, 123, 154].

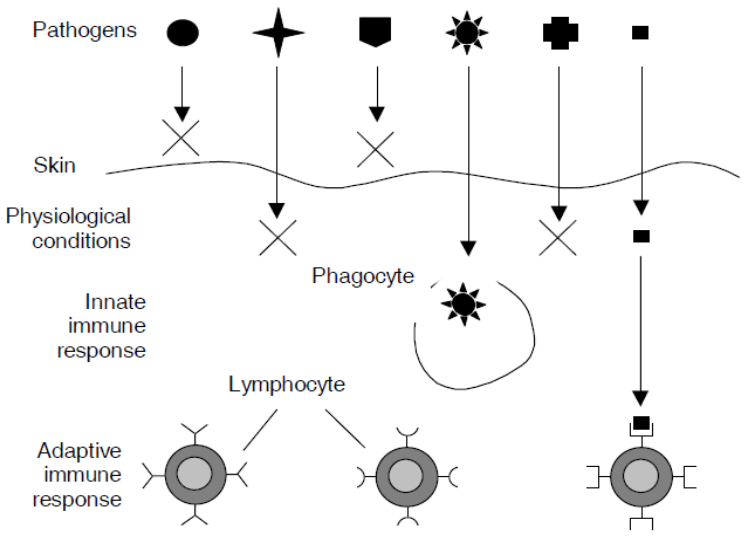


Figure 3.2. Multi-layer structure of the immune system

In literature many researchers deploy multilayer defence mechanisms inspired by human immune system multilayer capabilities. Example of those multi-layered defence models are [19, 34, 48, 53, 84, 156].

The main defensive layers of immune system include [5, 14, 55, 154, 155]:

1- Physical barriers: first and probably most effective layer, this include human skin which disallow thousands of invaders, also the respiratory system is defending human body from antigen. Physical layer defences include among others mucus, coughing and sneezing;
2- Physiological barriers: such as fluids, sweat and tears which contain destructive enzymes. Stomach acids also destruct most of the invaders ingested in food and water. The pH and temperature of the body present unsuitable life conditions for invaders;
3- Innate immune system: non-specific maximum immediate response to antigen stimulus, it has no memory. The innate immune system can be found in all life organisms;
4- Adaptive immune system (also known as acquired immune response): If a pathogen skip all above layers, it will be handled by the adaptive immune system which is a specific adaptable response to individual antigens.

3.2.2 Cells of the Immune System

The human immune system is made up of great number of cells that are originated in the bone marrow then circulates all over the body through the blood vessels. Although they are distributed around the human body and work independently but they are still cooperate chemically and effectively to protect human body [5, 13, 43, 153]. For efficient functioning different types of immune cells have different roles to play in the overall immune response. But generally speaking, immune cell are divided into two groups, the first group is responsible for general defence

whereas the other group are trained for responding to specific attack types [5, 154].

So, this great functionality of the immune system is clearly a direct reflection of the activities of 10^{12} cells of different kinds distributed all over the body working in parallel and precisely to specific objectives and communicate to each other using complex chemical signals with no central control [13, 154].

Figure 3.3 shows the structure of the immune cells.

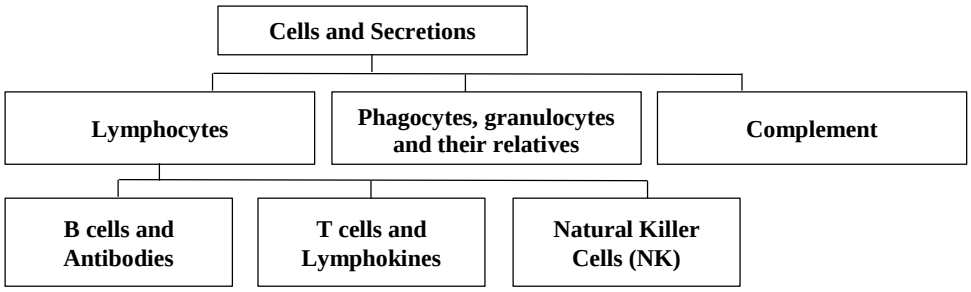


Figure 3.3. Structural division of the cells and secretions of the immune system [5]

3.2.2.1 Lymphocytes

Lymphocytes are small leukocytes that are considered as the main actors of the immune response. There are two main types of lymphocytes: B lymphocytes also known as B cells and T lymphocytes known for short as T cells.

The lymphocytes are activated only when interacted with antigens, The B and T cells express on their surfaces a chemical protein known as receptors highly specific for a given antigen (Ag).

The main role of the B cells is to produce antibodies (Ab) as a natural response to invasion, each B cell is programmed to produce a specific antibody. The T cells are matured in thymus, they are mainly responsible for attacking host infected cells. The T cells are divided into three subclasses: T helper cells (Th), cytotoxic (killer) T cells and suppressor T cells.

As illustrated in Figure 3.3 above there are another type of lymphocytes which is called the natural killer cells (NK). Unlike T cells, natural killer

cells do not need to recognize a specific antigen to start acting. These kind of cells are doing fundamental job and able to protect human body from great number of microbes especially in Tumors [5].

3.2.2.2 Phagocytes

The phagocytes are white blood cells capable of ingesting and digesting microorganisms and capable of presenting antigens to lymphocytes, so they called antigen presenting cells (APCs). The monocytes is a type of phagocytes playing important role at the beginning of the immune response. The neutrophils and eusinophils are also phagocytes with functions similar to those of the macrophages [5].

3.2.2.3 The Complement System

The complement system composes of a set of circulating plasma proteins that complement the role of the antibodies. When invaders detected each of its components, it promotes a cascade reaction results on binding and killing them [5].

3.3 How Immune System Protects the Body

The human body is protected by thousands of distributed cells work in parallel yet in cooperative way, with the only objective of reaching and eliminating antigens.

Figure 3.4 describes in brief the basic response of the immune system to the invaders as follow [5, 9, 11, 56]:

1. Antigen Presenting Cells (APCs) roam the body and process the pathogen, they find and fragmenting antigen into peptides displayed on their surfaces;
2. Pieces of these peptides are joined to major histocompatibility complex (MHC) molecules and are displayed on the surface of the cell. Other white blood cells, T cells, have receptor molecules that enable each of them to recognize a different peptide-MHC combination;

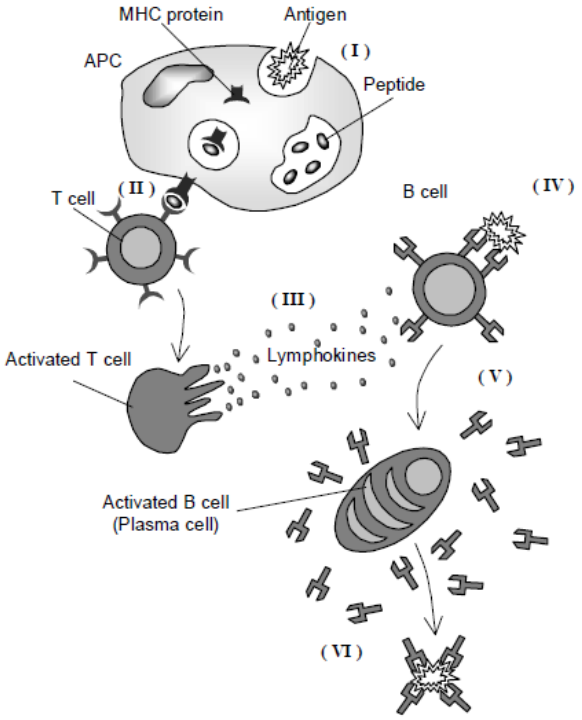


Figure 3.4. How immune system protects human body [5]

3. T cells activated by that recognition then divide and secrete lymphokines;
4. The B cells, which also have receptor molecules of a single specificity on their surfaces, respond to those signals. Unlike the receptors of T cells, B cells can recognize parts of antigens without MHC molecules;
5. When activated, the B cells divide and differentiate into plasma cells that secrete antibody proteins;
6. By binding to the antigens they find, antibodies can neutralize them or precipitate in their destruction by complement enzymes or by scavenging cells;
7. Some T and B cells become memory cells that persist in the circulation and boost the immune system's readiness to eliminate the same antigen if it presents itself in the future.

3.2.3 Adaptive Immune System

Adaptive immune system or acquired immune system is a distributed detection system with high abilities of learning, classification and pattern recognition [107] to name some of its characteristics targeted by researchers whom concentrated for decades on adaptive immunity before they are recently realized the important role of innate immunity and started modelling cooperative systems reflecting the cooperation and integration between innate and immune subsystems.

Adaptive immune system is developed through human life allows the body adaptively detect then neutralize or destroy unlimited number of specific invading pathogens, thus it is provided antigen-specific response even for infectious substances never encountered before [8, 40, 118]. Since microbes developed rapidly, they can often overcome the innate immunity, the body's originally programmed defence mechanisms that provide general protection, then they faced by the adaptive immunity which possess longer defence mechanism for specific targets [118].

Adaptive immune system consists of two kinds of lymphocytes B- and T-cells, lymphocytes are small independent detectors that circulate through the body in the blood and lymph systems and considered as main actors of the acquired immune response, these white blood cells are responsible basically for recognizing pathogens and neutralize and eliminate them [8, 19, 23, 54, 107]. Lymphocytes function as small independent detectors that circulate through the body in the blood and lymph systems.

B- and T-cells express proteins on their surfaces acting as detectors capable of interacting with specific antigen types. T-cells are protecting the body from attacking its own cells using negative selection algorithm, in this algorithm immature detectors are compare to self-patterns, those which respond to own cells of the body will be killed, others are start to be a mature detectors [22, 55, 107, 111].

As illustrated in Figure 3.5, antibodies are continuously compared to non-self patterns; those which match with high affinity will be cloned, detectors not match with antigen for certain time will be destroyed. The ability to detect different kind of pathogens requires a huge diversity of lymphocyte receptors, to ensure diverse type of detectors for better coverage, antibodies copy themselves with minor differences, this process called clonal selection algorithm [54, 111].

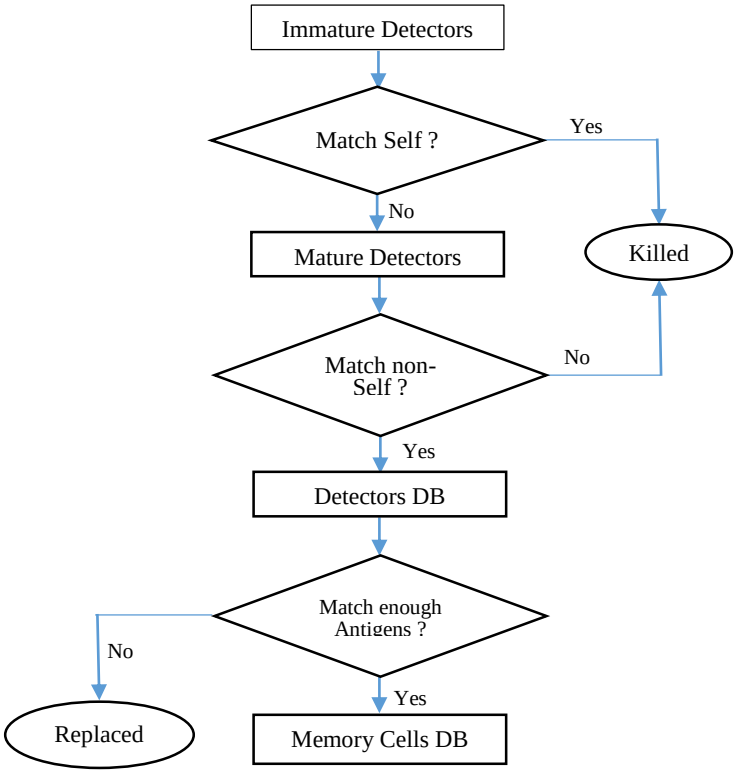


Figure 3.5. Detectors generation process [19]

Antibodies matching enough number of antigens in its life time will be added to memory cells database; this will help adaptive immune system to better respond to the same attacks in the future [19]. To ensure enough lymphocytes in the body to provide a complete coverage of all pathogen patterns, the lymphocytes continue circulating through the body and turnover continually to be replaced with new randomly generated receptors [11, 54].

3.2.4 Innate Immune System

Innate immune system is a natural resistance of the host to foreign invaders since this essential protection mechanism is present from birth yield to first line of defence system, the body is born with the natural ability to recognize different kind of microbes and immediately destroy them. Unlike adaptive immunity innate immunity uses comprehensive strategies to fight foreign antigens since it involves number of specialized white blood cells known as leukocytes responsible for recognizing and binding to common molecular patterns of disease [8, 11, 23, 118].

Innate immune system does not provide complete protection to the host and it does not confer long-lasting protection and it is not modified by repeated exposure and it doesn't adapt or learn from previous attacks [8]. The acquired immune system does not act independently to eliminate foreign invaders; both innate and adaptive immunity work together for the ultimate goal of protecting human body. Moreover, intensive research on biological immune system prove that the innate immunity occupied central role in the immune response and innate immunity plays a crucial role in the activation of the adaptive immune response [1, 12, 14, 154, 157]. Since no organism with only adaptive immune system, some research urges that there is no sense to build AIS with no innate immune capabilities [23].

One of the important features of the innate immune response is its rapid and quick response to invaders, unlike adaptive system which takes time to respond. Without a quick innate immune response, pathogens entering human body and multiply then it will become difficult to control and eliminate them [154].

For decades, research was focused only on adaptive immunity and AISs is largely been inspired by the adaptive immune system [1, 64, 89, 157], fortunately there is a notable interest in the innate system, as it is started

to provide some of the answers to the problems associated with the theories of adaptive immunity [12].

Table 3.2 shows the main properties of innate immune system.

Table 3.2. Main properties of innate immune system

Property	Explanation
First layer (line) of defence [8, 14, 108, 118, 151]	When antigen invade human body, the innate immune system is the first one to generate a response and provide rapid first line of defence, this will prevent many types of infections to enter and give time to adaptive immune system to be ready for more specific response.
Triggers adaptive immune system [14, 64, 151]	Innate immunity involved in the activation of the adaptive immune response, so the control of the adaptive response is firmly in the innate immune system.
Not adaptable [9]	Innate immune system does not adapt during human lifetime and remain the same every time.
Has no immunological memory [108]	Innate immune system has no immunologic memory and cannot learn unlike adaptive system, however some studies suggested that innate immune system has memory too [65].
Non-specific response [1, 8, 9, 14, 108, 158]	Innate response is not specific to particular pathogens, rather it responds in a generic way.
Responds according to general properties [9, 14, 108]	Innate immune response is react to general classes of pathogen and it focuses on class features, while adaptive system focuses on individual features.
Immediate maximal response [108, 154, 158]	Innate immunity immediately targets any invaders enters the body with its all available army.
Responds rapidly [118]	Innate immune system provides a rapid response to infections
Responds the same way every time [8, 108]	The innate immune system is an unchanging mechanism of protection.
Not long lasting response [8, 108, 158]	Innate system does not confer long lasting protection response.
Interact with adaptive [1, 14]	Both systems do not act independently, but in contrast, they work cooperatively to eliminate foreign invaders.
Non-complete protection [8]	Innate immune system is not capable of providing a complete protection.

Over the last decades, many researchers described the important role of the innate immune system as a co-partner with the adaptive immune system in protecting human body, and tens of research papers with suggesting different models and frameworks concentrating on innate immunity have been proposed. The following section shows examples of models and frameworks proposed in literature.

For example, Jamie Twycross and Uwe Aickelin [1] reviewed current immune system research with more focus on innate properties then they proposed innate conceptual framework with the aim of outlining meta-framework models of innate immunity.

Hosseinpour and the team [60] presented an intrusion detection system architecture based on the artificial immune system concept. The proposed framework used an innate immune mechanism through unsupervised machine learning methods to primarily categorize network traffic to “self” and “non-self” as normal and suspicious profiles respectively before adding adaptive immune system as a distributed structure which showed better self-improvement comparing to centralized mode.

Twycross [89] suggested that the importance of the innate immune system in AIS research is not reflected in literature, and he argued that the incorporation of innate properties into artificial immune systems will enhance the performance.

In [131] Tedesco and others proposed a novel intrusion detection algorithm based on theoretical models of innate immunity with the aim of discovering packets containing novel variations of attacks covered by an existing signature base.

Krishnan [154] simulated a very simple model of innate immune response which discriminates between self and non-self objects.

3.2.5 Interaction between innate and adaptive immune systems

In literature both systems are covered widely but in many cases they characterized as two separate subsystems, this view does not reflect the wide perspective describing the immune system as a parallel distributed system composing of great number of cells, organs and molecules cooperate and interact for the ultimate goal of protecting human body, so the innate and adaptive systems interplay provides human body with high level of comprehensive protection [9, 12, 43, 89]. Neither innate nor adaptive immune systems act independently from the other, they work together in a very cooperative environment and roles precisely distributed between them [14, 124].

It is important also to note that innate and adaptive immune systems operate over a typical different timescales. The innate immune system

started the immune response instantly or after a very short time and take a small time scale reacting to invasion, unlike adaptive immune system which operates over a longer time period, and initiate a reaction after long period of time [43]

Although, as mentioned before, literature focused in decades on adaptive immune mechanism, but recently intense research has appreciated and highlighted the importance central role of innate immunity in the natural immune system response mechanism, this is being reflected in AIS research with many models and frameworks having both innate and adaptive subsystems.

For example, in [124] Twycross et al. proposes a multilayer complex biologically-authentic AIS model with the purpose of showing the value of considering the interaction of innate and adaptive immune systems when designing a realistic AIS model.

Stepney, Timmis and others [32] propose a multidisciplinary conceptual framework and applied to AIS model of control system for complex electronic and electromechanical systems that would profit from long term autonomous operation; The system contains direct analogues of different systems including an artificial immune system, which consist of innate and adaptive layers of cells; an innate layer to initiate and filter data from sensors of the robot, and an adaptive layer to monitor and adapt to problems signalled by the innate layer.

Whigham [123] proposes AIS framework based on analogies of innate and adaptive set of principles focusing mainly on rule and feature-based problem representation.

Other examples of proposed interacted systems between innate and adaptive immune systems can be found in Section 3.2.5 above, like in [1, 60, 89, 131, 154].

3.4 Algorithms of Immune System

The Artificial Immune System main algorithms are negative selection, clonal selection and immune network theory. Those algorithms compose the most popular theories of the AIS research. [22], [23] and [159] presented a very rich literature review on AIS main algorithms.

Beside the three main algorithms, there are several other areas of immunology have recently been reported in the literature to inspire the development of algorithms and computational tools, for example, humoral immune response, Danger Theory, dendritic cell functions and Pattern Recognition Receptor Model. However, these new areas are still immature and under continuous investigation and development [44]

In the following sections main algorithms of immune systems will be presented in details.

3.4.1 Immune Network Theory

Niles Jerne [71] has introduced the immune network theory in 1974. The main idea of the theory is that the immune system is maintained by an interconnected network of lymphocytes mainly B-cells interact chemically to ensure stability of the whole system [22, 23, 39, 159].

In artificial immune network (AIN) theory, a B-cell population is made of two sub-populations: the initial population which generated from raw training data for the purpose of creating B-cell network, and the cloned population which is used for antigen training. Antigens are then selected randomly from the training set and presented to the B-cell network area in which B-cells will try to bind with enough affinity to the antigen, so successful cells will be cloned and mutated. Newly created B-cells will be integrated to the network, two B-cells are connected only if the affinities between them exceed certain threshold [22, 39, 158].

As reviewed in Table 3.3 there are many researchers develop models and frameworks and inspired ideas from the concept of artificial immune network theory.

Table 3.3. Immune network theory in literature

Reference	Description
Jerne, (1974) [71]	Described the main theory and ideas on immune network, it is also reviewed researchers efforts in developing models for solving the problems in various engineering applications.
Timmis et al., (2000) [162]	Proposed an artificial immune system using immune network theory to perform data analysis task. Artificial recognition ball (ARB) used to represent B-cells. Two B-Cells are linked together if the affinity between two ARBs is below a network affinity threshold [22, 159].
Timmis and Neal, (2001) [163]	Proposed a resource limited artificial immune system based on immune network theory. The main enhancements in this model comparing to Timmis model in [162] are the fixed total number of B-cells presented in artificial recognition ball (ARB) with centralized control. The cloning and Mutation process and the interactions between lymphocytes are done only at the ARB level [22].
De Castro and Zuben, (2000) [100]	Presented the aiNet model for data analysis tasks while antibodies are generated using Euclidean distance algorithm. In proposed system the immune network structure is not included in the antibody cloning selection process, the network cells are represented exactly as in AINE model [22, 159].
Castro and Timmis, (2002) [96]	Presented in details a real hierarchy of aiNets based model. The main contribution to the aiNet model was the proposed stopping criterion for the network interactive process and the introduction of an automatic hierarchical method to generate a tree of aiNets capable of detecting clusters with less-uniform characteristics.
Wierzchon, (2002) [101]	Proposed an interesting model combining the main ideas of aiNet and AINE with notable emphasize on self-organizing abilities i.e. the use of minimal number of control parameters [159].
Luh and Liu, (2004) [164]	Developed a reactive immune network for mobile robot learning navigation strategies within unknown environments. A modified virtual target method is integrated to solve local minima problem.
Neal et al., (2001) [165]	Proposed the system framed as self-stabilizing artificial immune system for determining time varying data using resource limited artificial immune system. The difference between this algorithm and the one in [163] is that there is unlimited number of resources are available.
Secker et al., (2003) [166]	Presented a model for email classification named as artificial immune system for e-mail classification. The proposed model intended to differentiate between interesting and non-interesting emails, It is capable of continuous learning for the purpose of two class classification and used for the task of electronic mail sorting [22, 23].
Alonso et al., (2004) [167]	Proposed a new approach to model an agent that plays the iterated prisoner's dilemma (IDP) based on the aiNet model. The agent structure consists of two immune networks components, recognition AIN and a decision AIN. The main improvement to the aiNet is the mechanism the network uses to add B-cell to the memory.
Tian et al., (2006) [168]	Proposed a modified version of aiNet algorithm to solve function optimization problems. This model suggests some improvements to aiNet like: the searching radius is a variable parameter depending on the number of the generations in which a cell survives, reserve the cell with the largest fitness and last the expanding rate is controlled to maintain the diversity of the network.
JiaLv et al., (2007) [169]	Proposed an algorithm for multimodal function optimization. To overcome the problem of premature convergence phenomena and unsatisfying searching precision when applying artificial immune system, the improved chaos immune network is used. For premature convergence, stopping criterion is used and searching accuracy is improved by using chaos variable.
Wenlong Huang et al., (2008) [170]	Proposed an immune kernel clustering network which works as a combination of artificially developed immune network and the support vector machine. Immune cell is divided in subparts by the antibody and each subpart is mapped into high dimensional feature space and each antibody neighborhood is regarded as a support vector hyper sphere.

3.4.2 Negative Selection Algorithm

The negative selection algorithm was first presented by M. Ayara et al. [160], the theory which explains how immune system detects antigens without reacting to its own cells.

Receptors are produced in a pseudo-random genetic rearrangement process during the generation of T-cells, then undergo a filtering process in thymus, this process is named as negative selection. In this process, lymphocytes respond to self-cells will be destroyed and only those not reacting will be allowed to leave thymus as matured T-cells circulating throughout the body to contribute in immunological system and eliminate foreign invaders [8, 14, 22, 23, 111, 158, 161].

It is not a surprise that negative selection algorithm is used frequently in literature in anomaly detection and pattern recognition systems, this is due to number of properties equipped with negative selection algorithm [62]:

- No prior knowledge of intrusions is necessary;
- Detection is probabilistic thus a complete repertoire of detectors will not be generated and only set of detectors will cover all possible non-self patterns;
- The detection scheme is inherently distributable;
- If one site is compromised, others would still be protected;
- The detector set protects the self-set against change and vice versa.

To date, researchers are inspired real-world solutions and applications from this phenomenal biological theory which gone through prodigious evolution [39]. When implementing negative selection algorithm originally, one limitation could arise resulted in an undetectable abnormal patterns, this is called holes [56]. Another reported limitation of this algorithm is that it is very time consuming this is due to the long time needed to produce detectors [171].

Table 3.4 below reviews the progress of the negative selection algorithm and provides examples of usage of this theory to solve real-world problems.

Table 3.4. Negative selection algorithm in literature

Reference	Description
M. Ayara et al.,(2002) [160]	Reviewed and investigated the usefulness of the negative selection metaphor as a human immune inspired system. The research provided a new immune system architecture based on negative selection algorithm and various procedures to generate detectors for the negative selection algorithm are reviewed and compared in terms of time and space complexity for the production of competent detectors.
S.Forrest et al., (1994) [172]	Described and reviewed a negative selection algorithm and described detectors generation and mutation where detector set are randomly generated by creating candidates and checks those elements which have self-data and destroy them.
Ilhan Aydin., (2010) [173]	Proposed a new method named as Chaotic-based hybrid negative selection algorithm. The algorithm showed very encouraging results for anomaly detection application.
Luther, Katja, et al.,(2007) [111]	Presented a cooperative intrusion detection approach inspired by biological immune system principles and P2P communication techniques to develop a distributed anomaly detection scheme. A dynamic collaboration between individual artificial immune system agents to address the well-known false positive problem in anomaly detection is utilized. The AIS agents use a set of detectors obtained through negative selection during a training phase and exchange status information and detectors on a periodical and event-driven basis, respectively.
Maoguo et al., (2012) [174]	Presented an efficient negative selection for anomaly detection. Self-detector are generated using extra training. Main motive of extra training is to eliminate self-samples and reduce the cost of computation at training stage. Self-region coverage is also improved by it.
K.Lgawa et al., (2009) [175]	Proposed an algorithm called as artificial negative selection classifier. Initially negative selection algorithm is not able to solve the problem of over fitting and over searching. So, the algorithm overcome these problems and increases the application area to multiclass classification.
L.Gonzalez et al.,(2004) [176]	Proposed a self-adaptive negative selection technique for anomaly detection uses self-adaptive techniques for constraint tuning. The main algorithm is divided in to two phases: the primary population generation and the growth of the population.
D. Dasgupta et al., (2004) [98]	Proposed a negative selection algorithm investigated for fault detection in man-in-the-loop aircraft operation. The detection algorithm uses body-axes angular rate sensory data exhibiting the normal flight behavior patterns, to generate probabilistically a set of fault detectors that can detect any abnormalities in the behaviour pattern of the aircraft flight.
Fernando et al.,(2004) [177]	Proposed a general framework for analysing different positive and negative detection schemes in the context of approximate matching and took anomaly detection application as an example for describing the framework functionality.
Xiaoshu Hang et al.,(2005) [90]	Proposed a novel approach of applying both positive selection and negative selection to supervised learning for detecting both normal and abnormal behavior. The system learns the patterns of the normal traffic via co-evolutionary genetic algorithm inspiring from the positive selection algorithm, and then generates synthetic samples of the anomaly class based on the negative selection algorithm.
Forrest et al., (1994) [82]	Proposed a negative selection algorithm based on the principles of self/non-self discrimination in the human immune system.
Sadeghi et al., (2013) [127]	Proposed an anomaly detection architecture based on negative selection. The system is intended to increase the speed of intrusions detection by reducing the number of the detectors, this accomplished by two techniques, clustering and

	updating the detectors. The experimental results show that the proposed algorithm increases the detection speed by approximately 50%.
Shen et al., (2012) [129]	Proposed AIS based intrusion detection system with Rough Set feature selection algorithm using negative selection algorithm, Feature selection algorithm to reduce the complexity of the system is used.
Gonzalez and Cannady, (2004) [176]	Presented a self-adaptive negative selection approach for anomaly detection application, the self-adaptive techniques is used for parameter tuning. The algorithm is composed of two phases generate the initial population and the evolution of the population.
Igawa and Ohashi, (2008) [175]	Proposed a multi-class classification negative selection algorithm named artificial negative selection classifier. Here negative selection algorithm and clonal selection mechanism are combined to solve issues that prevent negative selection algorithms from being applied to classification problems. These issues are like random searching, over fitting, and incomplete information.
Igbe and Saadawi (2018) [137]	Proposed a novel anomaly detection technique for insider threat detection using an ensemble consisting of multiple instances of an artificial immune system based on negative selection algorithm. The ensemble learns from normal user activity profiles during the training phase and then attempts to predict anomalies in new incoming user activity profiles. A proposal combined multiple NSA instances to make one single prediction unlike using standalone NSA.

3.4.3 Clonal Selection Algorithm

The clonal selection theory, principle or algorithm was first proposed by Burnet [70] and was inspired generally by the adaptive immunity, and it describes the very basic features of an immune system response to an antigenic stimulus [5, 8, 22, 39].

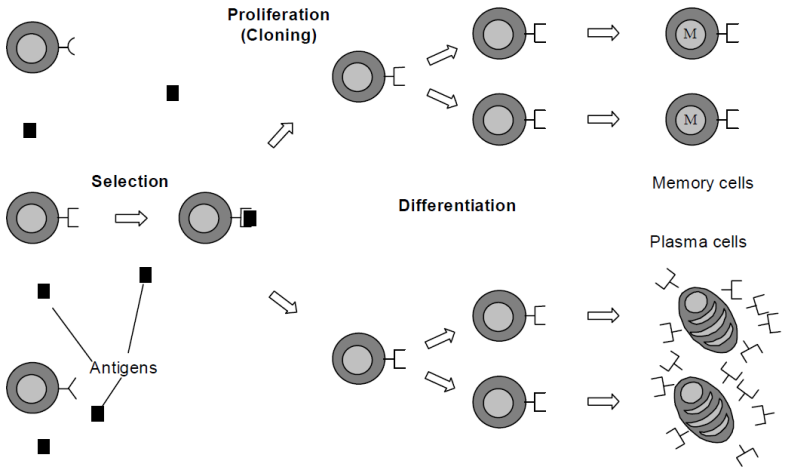


Figure 3.6. Clonal selection algorithm

The main idea of the clonal selection algorithm is that only cells or antibodies recognize the antigens will be able to proliferate and selected against those which do not [5, 22]. The algorithm describes the process of comparing detectors to a population of cells and only those recognize the abnormal patterns will be selected and cloned.

As illustrated in Figure 3.6, lymphocytes are proliferating then differentiate into either plasma cells, which are the most active antibody secretors, or into long-lived memory cells. To keep up with diverse set of detectors, the detectors cloned themselves with little differences [5, 111, 158].

In summary, the clonal selection algorithm is based on the following processes [112]:

- Holding a set of memory cells;
- Selection and cloning of the most stimulated antibodies;
- Re-selection clones proportionally to the affinity with the antigen;
- Removal of unstimulated antibodies.

Table 3.5 below reviews the progress of the clonal selection algorithm and provides examples of usage of this theory to solve real-world problems.

Table 3.5. Clonal selection algorithm in literature

Model	Description
Chan et al., (2013) [135]	Presented and explained a clonal selection classification algorithm which has been successfully implemented to classify the data for a network intrusion detection problem. The main problem taken into consideration is the classifier problem of network intrusion detection by applying anomaly based approach. To classify the problem dataset a clonal selection classification algorithm worked in a negative selection algorithm base through artificial immune system is been applied and verified.
M. Gong et al., (2007) [178]	Proposed an improved clonal selection algorithm based on CLONALG, the system used logistic chaotic sequence to generate the initial antibody population, while the hyper mutation adopts self-adaptive chaotic mutation.
Vincenzo Cutello et al., (2006) [179]	Described opt-IMMALG (optimization immune algorithm) and proposed some changes and modifications to the algorithm. The main changes are the use of real codes in place of the binary string and inversely proportional hyper mutation operator is used in place of hyper mutation.
X.Bian et al., (2005) [180]	Proposed an adaptive clonal selection algorithm for optimal phasor measurement unit (PMU) placement. The system proposed solution to fix the probabilities of hyper mutation and recombination operators of the CLONALG algorithm and the number of the cycle supplement population.
Kim and Bentley, (2002) [181]	A new dynamic clonal selection algorithm was introduced as a step towards an artificial immune system that is better able to deal with a real environment. It described in details main features of immune system implemented in this algorithm like central tolerisation, distributed tolerisation, co-stimulation, affinity maturation and memory.
Purbasari, A. et al., (2013) [182]	Proposed an agent based immune system approach using clonal selection features. The communication and performance of agents is define using UML diagrams.
Hongwei Dai et al., (2014) [183]	Proposed Bi-direction quantum crossover-based combined by clonal selection algorithm to increase the performance. The system is motivated by quantum

	theory in which energy is released when atom moves from higher to lower energy level and energy is absorbed when atom moves from lower to higher energy level.
Yong Peng et al., (2015) [184]	Proposed a new hybrid learning clonal selection algorithm, which is a combination of baldwinian learning and orthogonal learning approaches. For global search baldwinian learning is used and for local search orthogonal learning is used. This algorithm overcomes the problem of hyper mutation operator which is affecting performance in complex problems.
Karakasis et al., (2006) [28]	Proposed a hybrid evolutionary technique for data mining tasks, which combines the clonal selection principle with gene expression programming. The proposed algorithm used the new concept called data class antigens to represent a class of data. The CLONALG extension algorithm is used to represent the clonal selection mechanisms. In the present algorithm, among other new features, a receptor editing step has been incorporated. The test results show very satisfaction prediction accuracy.
Xian et al., (2005) [27]	Proposed a framework of anomaly detection system using unsupervised fuzzy clustering method based on clonal selection algorithm. The intention is to obtain the global optimal clustering with clonal operator which combines the evolutionary search, global search, stochastic search and local search. And then detect abnormal network behavioral patterns with fuzzy detection algorithm.

3.4.4 Positive Selection Algorithm

Positive selection algorithm is the process of eliminating useless lymphocytes and rescuing only efficient cells, this process is thus control the survival and differentiation of receptors [5, 40]. Through positive selection, only T cells able to recognize MHC will be kept others will be discarded [14, 123].

Researchers are using the concept of positive selection frequently in modelling solutions to engineering problems. In literature many examples can be demonstrated, such as the use of positive selection algorithm in network anomaly detection by Tie Shan [185] in which a positive selection detector generation process presented in details. Also Luther et al. [111] implemented a simple and effective detection solution using positive selection for detecting abnormal network packets. Hang et al. [90] uses genetic algorithm approach inspired by positive selection algorithm in generating normal patterns samples and uses negative selection algorithm for generating abnormal patterns samples.

3.4.5 Danger Theory

The Danger Theory was first introduced by Polly Matzinger in 1994 [186, 187] which in concept suggests that the immune system is responding only

to danger signals not to all non-self invaders. Matzinger argues that no need to react to all non-self, example of that, immune system doesn't react to food although it is foreign invader. The main idea of danger theory is that only invaders categorized as dangerous will induce the generation of danger signals [172, 188, 189]. So the theory supports discrimination between "some self sets" from "some non-self sets" but react only to danger ones [44, 190].

In literature many AIS researchers design and model artificial immune systems using danger theory, Table 3.6 shows different examples of research work of AIS using danger theory.

Table 3.6. Danger theory in literature

Research	Idea
Behrozinia et al., (2013) [191]	Proposed an anomaly detection system inspired by biological immune system using the concept of danger theory. Danger signal is used in intention of reducing the false alarms this is achieved through KNN classifier.
Mahboubian et al., (2012) [172]	Proposed an alert fusion model inspired by artificial immune system theory which used to fuse the generated alerts by the IDSs in a computer network. Inspired by the human immune defence mechanism system, this model uses danger theory with the attempt to aggregate alerts based on a general set of predefined rules, and also to reduce the false alarms.
Lebbe et al., (2008) [189]	A research of an artificial immune system model to employ in secure routing in wireless mesh networks (WMN) is proposed as a continuation of the previous effort. The objective of this enhancement was to improve and extend the algorithm with more achievable danger levels and to introduce responsible parameters and model danger in WMN.
Mihaljevic et al., (2006) [40]	Proposed a recommender system model based on artificial immune system. The system provided a web portal news article recommender based on artificial immune system inspired by danger theory. System knowledge represents learned user preferences using implicit tracking of user actions and adapts to evolution of user's opinion and expresses results in a readable personalized recommendation list format.
Aickelin et al., (2003) [134]	Proposed a next generation intrusion detection system using artificial immune system based on danger theory. The aim of this research is to investigate the correlation and to translate the danger theory into the realms of computer security, thereby creating AIS that are no longer limited by self-nonself discrimination.

3.4.6 Co-stimulation

Co-stimulation is the concept of second signal which is used to closely regulate B-cells in order to prevent uncontrolled immune response, and mainly to prevent B-cells from incorrectly reacting against self cells.

The main purpose of the second signal is to redetect a non-self so to minimize false alarm [56, 122]. The active B-cell receives two signals telling that it bound to pathogen not self cell, this process is illustrated in Figure 3.7 below [118].

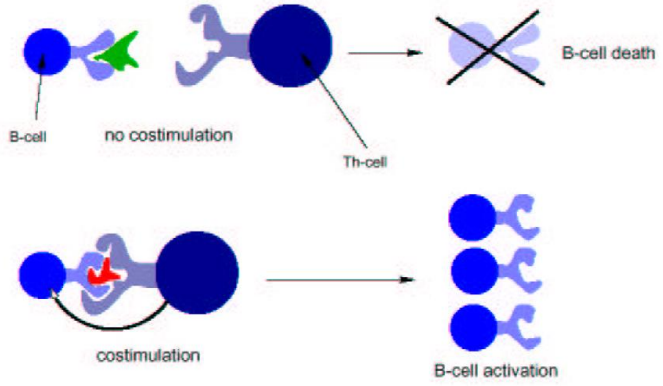


Figure 3.7. Co-stimulation process [118]

Many researchers used the concept of co-stimulation in modelling and designing their research solutions, for example: [56], [181] and [185].

CHAPTER FOUR

A NOVEL ARTIFICIAL IMMUNE SYSTEM FRAMEWORK FOR NETWORK SECURITY SYSTEM

4. A Novel Artificial Immune System Framework for Network Security System

4.1 Overview

This chapter describes the main components and the work on developing a multilayer network defence framework that simulates human immune system capabilities and response to anomalies and invaders.

In the proposed system it was intended to capture the most recent advantages of the research of artificial immune system taking into account a number of suggestions as a way forward to assist AIS researchers to take this research area to the next level.

The proposed system combines different intelligent techniques to enhance the detection capabilities of the system. The ultimate goal for network defence systems generally is to protect network from invaders and malicious activities, this can't be achieved without an accurate detection mechanism able to detect intrusions with high detection rate and low false alarm rate.

As reviewed before in this thesis, and after decades of deep research on AIS, many researchers have argued that AIS models should incorporate innate immune system with adaptive immune system, this will make it more realistic and help bring more theories and tactics to the field. Moreover, tens of research papers showed that combining both innate and adaptive components in a single AIS model resulted in more effective systems, especially in computer security applications having both innate and adaptive immunity is useful since both systems use different defence strategies [12, 14, 43].

Another important suggestion is to build AIS models together with other computational intelligence techniques such as neural networks or fuzzy logic systems. The main advantage of using hybrid intelligent systems is

to avoid individual limitations, also to benefit from the capabilities of those systems that may be advanced in specific areas only.

As illustrated in chapter one, this research is aiming to overcome some of the intrusion detection system limitations, such as high false positive rate and inability to deal with unknown patterns. In this project it was intended to build in-depth adaptable security mechanism capable of learning by themselves and defend networks by fighting intruders in different layers. The proposed defence system has capabilities and techniques of both IDS mechanisms, i.e. anomaly detection and signature based.

4.2 Framework Description

Figure 4.1 shows a proposed novel multi-layered defence system inspired by biological immune system, the proposed framework composes of four main components, the input unit as a preparatory component then the two layers of defence the innate and the adaptive components in addition to the co-stimulation component which is considered part of the adaptive layer.

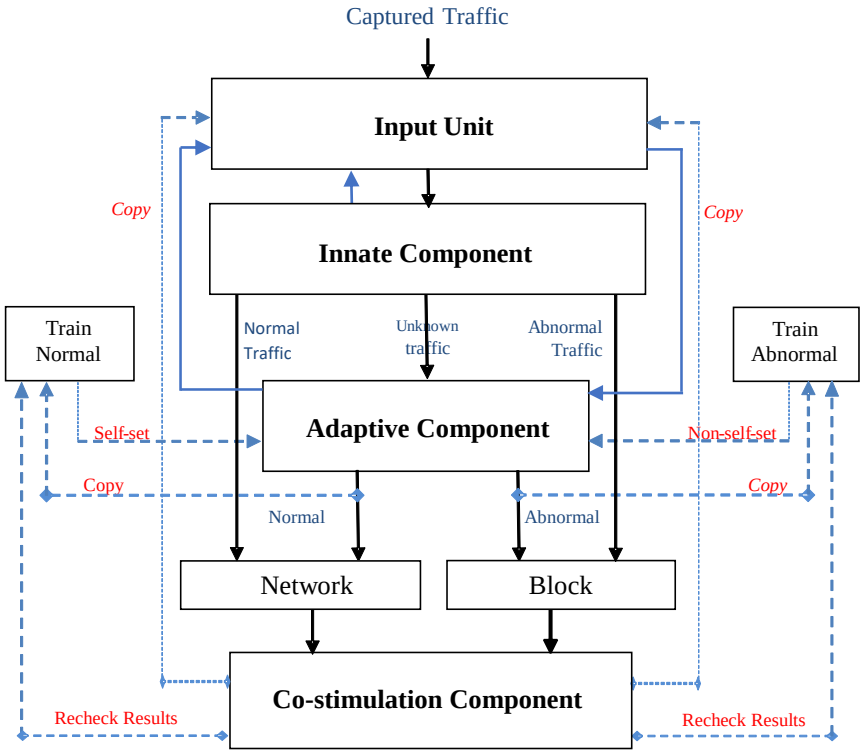


Figure 4.1. A multilayer network defence system framework

As illustrated in Figure 4.1, captured network traffic will enter into the input unit in which the following processes are accomplished:

- Loading data into database;
- Extract features and attributes from the captured traffic;
- Add more rules to the knowledge base;
- Prepare data to be entered into innate layer in a suitable format;
- Preparing a lookup table with connection number and time stamp;
- Prepare parameters and variables;
- Delete duplicated records of the dataset (for test purposes only).

The input unit will copy all entered traffic and passes only lookup table with all needed attributes for innate and adaptive layers. The traffic first sent to the innate immune system component as a first layer of defence in a dataset format labelled with connection number and time stamp for each connection. The innate layer uses fuzzy expert system to categorize traffic into one of three categories i.e. normal, abnormal or unknown traffic. The normal traffic will be ignored and allowed to pass to the network without further delay or investigation, the abnormal traffic will be blocked and not allowed to reach network, the third category is the unknown traffic, in other words, the traffic that the innate system could not judge whether it is normal or abnormal, and here the innate component calls the adaptive layer of the immune system for further investigation. The innate categorization decision will be sent back to input unit containing only connection numbers and time stamp for each category, then input unit will react as follow:

1. For normal traffic: input unit will send original data to network
2. For abnormal traffic: input unit will not allow traffic to pass
3. For unknown traffic: an extracted table will send to adaptive containing only connections numbers and time stamp for only connections categorized as unknown in innate layer.

The innate layer categorization and decision making is performed in a fast manner and preserve the feature of the innate mechanism in increasing the speed of the overall network defence performance.

As mentioned above, traffic considered unknown will pass to the second layer of defence, the adaptive layer, experiments show that only around 20% of the overall traffic reached adaptive layer for further inspection, this will definitely reduce overhead of the adaptive layer, and since the adaptive detection mechanism is totally different from the innate way of defence this will help better reaction to those not detected by first layer.

The adaptive layer discriminates self-sets from non-self-sets, self-sets will be ignored and allowed to enter into network and copy of this traffic will be used as trained data to produce more self-sets, whereas the non-self-sets will be blocked and denied to access network and copy of this traffic will be used as trained data for producing antibodies for non-self-sets. The training process for both normal and abnormal traffic is being conducted offline and could be in any other separated PC or network.

The adaptive decision will be either to block traffic for abnormal ones or to allow it to pass to the network for legitimate traffic. The adaptive component will feed the input unit back with its decision in a small extracted table, the input unit will allow the original traffic categorized as normal using connection numbers and time stamp to pass to the network and block other traffic categorized as abnormal.

To review and enhance the detection capabilities of the adaptive component another layer called co-stimulation for rechecking the output of adaptive layer was added, results will be added to training PCs for training both self and non-self-sets to better react to same connections in the future. Co-stimulation in biology or the second signal decreases false positive rates since it rechecks the cells categorized as abnormal by adaptive detection mechanism. Here in the proposed defence system the

same concept of co-stimulation is used, but for both normal and abnormal connections.

4.3 Innate Component

As mentioned earlier, most AIS research focus has been on the adaptive immune system and only recently innate immunity has found some consideration, many applications and frameworks using adaptive immunity are available throughout the literature, and in contrast those using innate immunity can hardly be found [1, 124, 154]. In the proposed framework an integrated system with levels of interacting defence components is presented including both innate and adaptive immunity, and the role of the innate immunity as the instigator of the adaptive immunity system was explored.

Innate immune layer has been formulated using fuzzy expert system with the aim of taking decisions based on pre-determined expert knowledge that may incorporate uncertain information. The system is designed to fulfil the well-known biological innate immune system properties which are divided into two main groups, the first group is related to general attributes of the innate system, whereas the second one is describing how innate responds to the antigen. The properties of the innate immune system have been described in details in chapter 3.

The properties related to general attributes are:

- First layer of defence;
- Triggers adaptive system to start its response;
- Not adaptable system;
- Has no memory, although some researchers suggested that innate system could have immunological memory [64].

The properties related to innate response are:

- Non-specific response;
- Responds according to general properties;
- Immediate maximal response;

- Responds rapidly;
- Responds the same way every time;
- Not long lasting response.

The proposed innate layer response highly reflects the properties of the human innate system in responding to antigen stimulus, it acts as a first responder to antigen to formulate the first layer that defend human body, it is also designed to classify attacks according to general properties and to network behaviour unlike the acquired immune response which is specific to certain attacks.

The system is designed to react to non-fuzzy inputs as well as uncertain connections using fuzzy expert system abilities to translate uncertain expert knowledge base into a decision making process and its known capabilities of converting human rules into mathematical formulations to be easily designed and implemented using computer programs.

The use of a fuzzy system is motivated by its capability to provide low solution cost for complex problems and the ability to translate uncertain expert knowledge into a decision-making process. Furthermore, it also has practicable memory requirements of look-up tables.

Fuzzy logic implementation is much simpler and its expected results are more accurate and does not need to design a specific mathematical model, it only requires practical understanding of the overall behaviour.

As shown in Figure 4.2 the input unit classifies network traffic into either crisp or fuzzy inputs, both inputs go through fuzzification process where fuzzy sets are defined and a degree of membership for crisp inputs are defined as well, then when passed through inference engine, fuzzy rules will be evaluated and output for each rule will be produced using rules stored in the knowledge base, those rules are collected and generated using network security experts knowledge and general traffic observations.

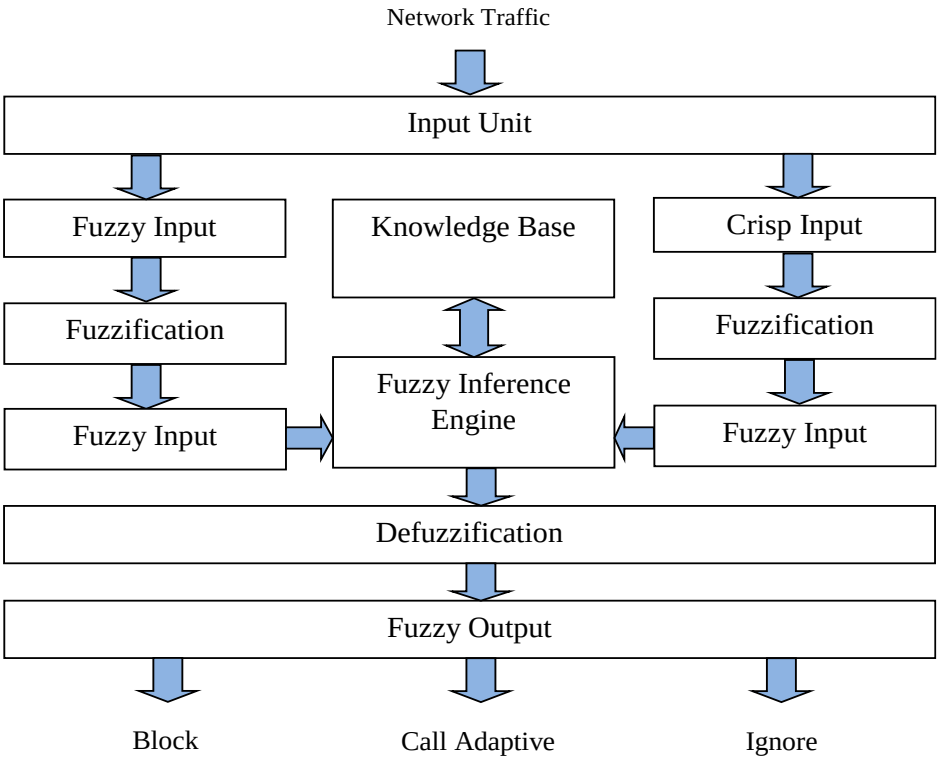


Figure 4.2. Innate immune layer using fuzzy expert system

In the defuzzification process the output decision will be taken after combining all outputs of all rules, the system will have one of three decisions i.e. ignore, block or call adaptive component.

Many fuzzy set shapes can be used i.e. triangular, rectangular, bell-shaped, gaussian, shoulder shaped, etc., in this research triangular fuzzy sets are used for simplicity. Using other shapes can be an area of study for further research.

Figure 4.3 shows an example of one of the fuzzy sets called *duration* and shows how lingual expressions like short, very short and long are mathematically described. In this research 22 features have been chosen from the 41 features of the KDD'99 dataset. Table 4.1 shows how the constructed fuzzy sets for the 22 chosen KDD'99 features and the determined scale for each.

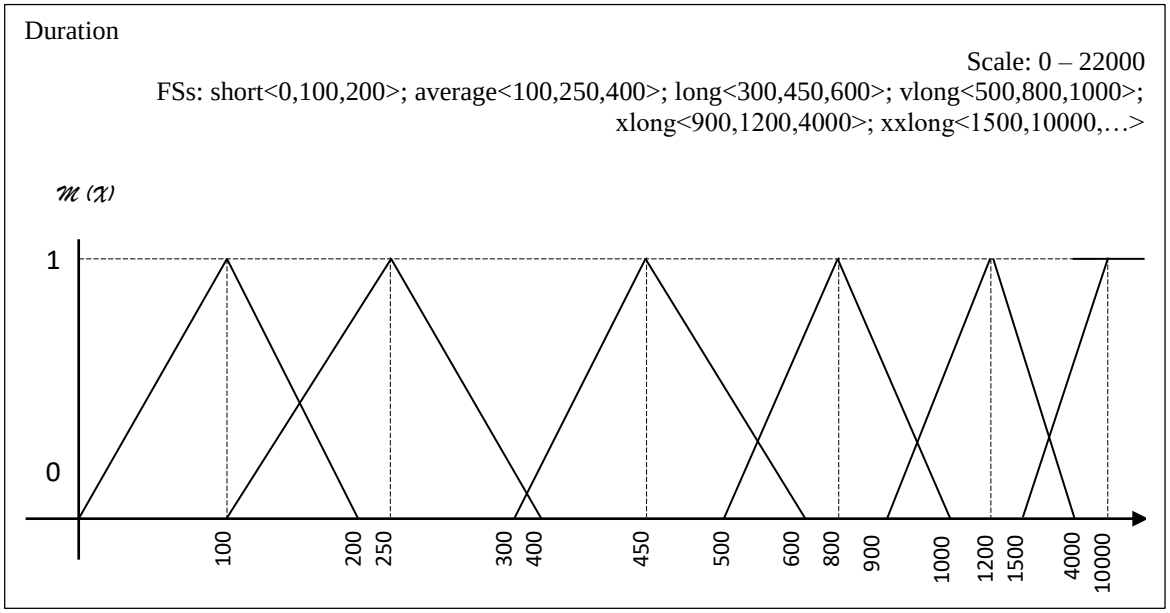


Figure 4.3. Fuzzy set for the 'Duration' feature

Table 4.1. Construction of fuzzy sets

No	Feature Name	Fuzzy Scales	Fuzzy Sets
1	Duration	0 – 22000	short<0,100,200>; average<100,250,400>; long<300,450,600>; vlong<500,800,1000>; xlong<900,1200,4000>; xxlong<1500,10000,…>
2	src_bytes	0 – 2000	vfew<0,75,100>; few<75,100,200>; average<150,250,300>; many<275,500,800>; xmany<600,1200,2000>; xxmany<1600,3000,….>
3	dest_bytes	0 – 10000	vfew<0,100,300>; few<200,350,500>; average<400,1000,3000>; many<2000,4000,6000>; xmany<5000,10000,…>
4	Count	0 – 520	vfew<0,25,50>;few<35,80,120>;average<100,200, 300>; many<280,350,400>; xmany<375,450,520>
5	srv_count	0 – 520	vfew<0,25,50>;few<35,80,120>;average<100,200, 300>; many<280,350,400>; xmany<375,450,520>
6	serror_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
7	srv_serror_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
8	rerror_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
9	srv_error_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
10	same_srv_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
11	diff_srv_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
12	srv_diff_host_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
13	dst_host_count	0 – 255	few<0,10,50>; average<25,60,100>; many<80,120,180>; xmany<150,200,255>
14	dst_host_srv_count	0 – 255	few<0,10,50>; average<25,60,100>; many<80,120,180>; xmany<150,200,255>
15	dst_host_same_srv_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.65,0.75>; xmany<0.70,0.80,1.00>

16	dst_host_diff_srv_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.65,0.75>; xmany<0.70,0.80,1.00>
17	dst_host_same_src_port_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
18	dst_host_srv_diff_host_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
19	dst_host_serror_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
20	dst_host_srv_serror_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
21	dst_host_rerror_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>
22	dst_host_srv_error_rate	0.00 – 1.00	vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>

4.3.1 Generating Rules

The general observations used in the fuzzy knowledge base are extracted by analysing the daily network traffic; an example of suspicious behaviour could be: high network traffic after 4 pm, a big number of traffic sent from a specific destination or an excessive number of ICMP messages. An example of legitimate network traffic is DNS and ARP requests, TCP three-way-handshaking connections or UDP broadcast messages.

A considerable amount of information are collected from experts and taken from known general network attributes, these information are formulated in IF-Then format and added to the knowledge base, below are examples of such information:

- 70% of small sized packets are attacks [192],
- Some Ports are frequently used by attackers, like 443, 135, 445, 137 etc.,
- Reserved or private IP addresses should not be seen in internet,
- Packets should never have a source or destination port set to 0,
- TCP packets should not use a destination address that is a broadcast address, because broadcasts are normally performed using UDP not TCP [192].

	1	2	3	4	5	6	7	8	9	10
Rule No	Duration	protocol_type	service	flag	src_bytes	dest_bytes	Land	wrong_fragment	urgent	Hot
R001	xlong	TCP	http		xxmany					
R002	vshort	ICMP	echo_i	SF	xmany					
R003		TCP		S0						
R004			netbios						>= 3	
R005		TCP					1			
R006	average	ICMP			xmany			> 0		
R007	short	TCP	http		xxmany	xmany				
R008	average	UDP	private					>= 3		
R009		TCP		RTSO						
R010		UDP								
R011	short	TCP	http	S1						
R012	short	ICMP	dhcp	ecr_i						
R013	short	TCP	SMTP		xxmany	few				
R014		ICMP		Echo_Request	vfew					
R015	xxlong	TCP	port 79							
R016		UDP	echo - private					>= 2		
R017		TCP	http							

Main Attacks | Other Attacks | abnormal behavior | normal profiles

Figure 4.4. Screen captured picture from knowledge base

Figure 4.4 shows captured screen picture from the knowledge base which consists of more than 3000 rules extracted from general behaviour, observations, expert's knowledge, studying 144 attacks and well known general network information.

4.3.2 KDD'99 Dataset

Most of the tests have been performed using corrected version of the well-known KDD'99 dataset which is a benchmark dataset well defined, organized and labelled to precisely evaluate the performance of intrusion detection systems, this dataset is based on the DARPA 1998 raw dump traffic including payload captured over a period of nine weeks on a local area network in Information System Technology (IST) group of Lincoln Laboratories at MIT University [193].

KDD dataset is the most comprehensive source of attacks with 37 attacks and normal traffic as well [16]. The KDD'99 as one of the few publicly available high quality datasets has become one of the most widely used datasets in the evaluation and benchmarking IDSs and provides the only labelled datasets for comparing IDS systems [194, 195].

KDD'99 dataset has a number of inherent problems, as illustrated in [15] and [16] the dataset is imbalance since two attacks Smurf and Neptune made up more than 70% of it, and these two attacks plus normal connections made up to 98% of the training dataset; KDD'99 dataset is

outdated and misses many of the new attacks [15, 194, 195] and also many connections of the dataset are duplicated (78% of the training set and 75% of testing set are exactly the same) [15, 195, 196]. Another criticism against DARPA benchmark that the test bed traffic generation software is not publicly available so it is not easy to determine how accurate was the traffic entered into the test system [195].

Hence, the need for a new labelled high-quality dataset has become essential in intrusion detection system. Although, there are other datasets available, like NSL-KDD, GureKDD and Koyot2006, but they never gained as much importance as the KDD'99 dataset [197]. Another publicly available dataset which is used to test anomaly detection systems is the University of New Mexico (UNM) dataset, this dataset records the syscalls made for a variety of UNIX process under normal and attack usage [89].

In this research a number of solutions applied for the purpose of overcoming the main drawbacks of KDD'99 dataset concentrating on having better test results, Table 4.2 below showed proposed solutions.

Table 4.2. KDD'99 drawbacks and proposed solutions

No	Darpa 1999 Drawbacks	Proposed Solution
1	Imbalance, since two attacks Smurf and Neptune made up more than 70%	Using samples from each attack, 500 or less connection for each attacks including added attacks. Also using the Corrected KDD'99 version which is more balanced.
2	Outdated and misses many of the new attacks	Added connection related to 144 attacks plus normal connection including the 37 attacks from KDD'99
3	Many connections are duplicated	The Input Unit is deleting the duplicated connections as one of its functions
4	The test bed traffic generation software is not publicly available	Testing KDD'99 samples before using them in experiments

In the main tests, corrected version of the KDD'99 dataset being used, unlike in 10% KDD, corrected version has more balance attacks distributions and has bigger number of attacks, i.e. 37 attack types [198]. To have more balanced traffic and to reduce the memory usage in the test only 500 connections or less was tested for each attack type and 5000 connections for normal connections, those sample connections are

randomly selected after the input unit eliminate duplicated traffic to overcome one of the KDD'99 dataset drawbacks. The system changes selected samples each time the test performed, the results showed later are the average rates from different tests generated.

For validation and benchmarking purposes three more tests were conducted using NSL-KDD dataset, the refined version of its predecessor KDD'99 data set.

Figure 4.5 below shows captured picture from the corrected KDD'99 dataset, the picture shows three different attacks and the values of the 41 features for each, it shows also at the end the labelling for each connection.

180,icmp,ecr_i,SF,1480,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,4,0.00,0.00,0.00,0.00,1.00,0.00,0.50,2,38,1.00,0.00,1.00,0.50,0.00,0.00,0.00,0.00,pod

200,icmp,eco_i,SF,18,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,4,244,1.00,0.00,1.00,0.25,0.00,0.00,0.00,0.00,ipsweep

210,udp,private,SF,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,26,5,0.00,0.00,0.00,0.00,0.19,0.12,0.00,255,5,0.02,0.89,0.13,0.00,0.11,0.00,0.76,0.00,satan

Figure 4.5. Corrected KDD dataset

Table 4.3. KDD'99 features and their representations

No	Feature	Explanation	In KDD	Type	Scale
Intrinsic attributes: these attributes are extracted from the headers' area of the network packets					
1	Duration	duration of the connection	Integer	Fuzzy	0 –22000
2	protocol_type	connection protocol like TCP, UDP or ICMP	Nominal	Crisp	
3	service	destination service like Telnet, FTP, IMAP, etc.	Nominal	Crisp	
4	Flag	connection status, the possible status: SF, S0, S1, S2, S3,OTH, REJ, RSTO, RSTOS0, SH, RSTRH, SHR *1	Nominal	Crisp	
5	src_bytes	bytes sent from source to destination	Integer	Fuzzy	0 –2000
6	dest_bytes	bytes sent from destination to source	Integer	Fuzzy	0 –10000
7	Land	if source and destination IP addresses and port numbers are equal then, this variable takes value 1 else 0	Binary	Crisp	0 – 1
8	wrong_fragment	sum of bad checksum packets in a connection	Integer	Crisp	0 – 5
9	urgent	sum of urgent packets in a connections. Urgent packets are packets with the urgent bit activated	Integer	Crisp	0 – 5

No	Feature	Explanation	In KDD	Type	Scale
Content attributes: these attributes are extracted from the contents area of the network packets					
10	Hot	sum of hot actions in a connection such as: entering a system directory, creating programs and executing programs	Integer	Crisp	0 – 15
11	num_failed_logins	number of incorrect logins in a connection	Integer	Crisp	0 – 5
12	logged_in	1 if successfully logged in; 0 otherwise	Binary	Crisp	0 – 1
13	num_compromised	number of "compromised" conditions - sum of times appearance “not found” error in a connection	Integer	Crisp	0 – 165
14	root_shell	1 if root shell is obtained; 0 otherwise	Binary	Crisp	0 – 1
15	su_attempted	if the su command has been used then 1 else 0	Binary	Crisp	0 – 1
16	num_root	sum of operations performed as root in a connection	Integer	Crisp	0 – 5
17	num_file_creations	sum of file creations in a connection	Integer	Crisp	0 – 5
18	num_shells	number of logins of normal users	Integer	Crisp	0 – 5
19	num_access_files	sum of operations in control files in a connection	Integer	Crisp	0 – 5
20	num_outbound_cmds	number of outbound commands in an ftp session	Integer	Crisp	0 – 5
21	is_hot_login	if the user is accessing as root or admin	Binary	Crisp	0 – 1
22	is_guest_login	if the user is accessing as guest, anonymous or visitor	Binary	Crisp	0 – 1

No	Feature	Explanation	In KDD	Type	Scale
Content attributes: these attributes are extracted from the contents area of the network packets					
23	count	sum of connections to the same destination IP address	Integer	Fuzzy	0 – 520
24	srv_count	number of connections to the same service (destination port number) as the current connection in the past two seconds	Integer	Fuzzy	0 – 520
25	serror_rate	% of connections that have “SYN" Errors- the percentage of connections that have activated the flag s0, s1, s2 or s3, among the connections aggregated in count	Real	Fuzzy	0.00 – 1.00
26	srv_serror_rate	% of connections that have “SYN" Errors - the percentage of connections that have activated the flag s0, s1, s2 or s3, among the connections aggregated in srv_count	Real	Fuzzy	0.00 – 1.00
27	rerror_rate	% of connections that have “REJ" Errors - the percentage of connections that have activated the flag REJ, among the connections aggregated in count	Real	Fuzzy	0.00 – 1.00
28	srv_error_rate	% of connections that have “REJ" errors - the percentage of connections that have activated the flag REJ, among the connections aggregated in srv_count	Real	Fuzzy	0.00 – 1.00
29	same_srv_rate	% of connections to the same service - the % of connections that were to the same service, among the connections aggregated in count	Real	Fuzzy	0.00 – 1.00
30	diff_srv_rate	% of connections to different services - the % of connections that were to different services, among the connections aggregated in count	Real	Fuzzy	0.00 – 1.00
31	srv_diff_host_rate	% of connections to different hosts - the % of connections that were to different destination machines among the connections aggregated in srv_count	Real	Fuzzy	0.00 – 1.00

No	Feature	Explanation	In KDD	Type	Scale
Content attributes: these attributes are extracted from the contents area of the network packets					
32	dst_host_count	count of connections having the same destination host	Integer	Fuzzy	0 – 255
33	dst_host_srv_count	count of connections having the same destination host and using the same service (having same port number)	Integer	Fuzzy	0 – 255
34	dst_host_same_srv_rate	the percentage of connections that were to the same service, among the connections aggregated in dst_host_count	Real	Fuzzy	0.00 – 1.00

35	dst_host_diff_srv_rate	the percentage of connections that were to different services, among the connections aggregated in dst_host_count	Real	Fuzzy	0.00 – 1.00
36	dst_host_same_src_port _rate	the percentage of connections that were to the same source port, among the connections aggregated in dst_host_srv_count	Real	Fuzzy	0.00 – 1.00
37	dst_host_srv_diff_host_ rate	the percentage of connections that were to different destination machines, among the connections aggregated in dst_host_srv_count	Real	Fuzzy	0.00 – 1.00
38	dst_host_serror_rate	the percentage of connections that have activated the flag s0, s1, s2 or s3, among the connections aggregated in dst_host_count	Real	Fuzzy	0.00 – 1.00
39	dst_host_srv_serror_rate	the percentage of connections that have activated the flag s0, s1, s2 or s3, among the connections aggregated in dst_host_srv_count	Real	Fuzzy	0.00 – 1.00
40	dst_host_rerror_rate	the percentage of connections that have activated the flag REJ, among the connections aggregated in dst_host_count	Real	Fuzzy	0.00 – 1.00
41	dst_host_srv_error_rate	% of connections to the current host and specified service that have an S0 error	Real	Fuzzy	0.00 – 1.00

Table 4.3 shows the 41 KDD'99 features and the features chosen among them as fuzzy, not crisp, and the scales for each of them. Then Table 4.4 shows other features added to those KDD features.

Table 4.4. More added features (not in KDD)

No	Feature	Format	Type
1	TCP_flag	Char	Crisp
2	max_packet_size	fixed Number Equals to 65535 bytes	Crisp
3	acknowledge_no	Integer	Crisp
4	no_of_ICMP_messgs	Integer	Fuzzy
5	Is_local_IP	yes – no	Boolean
6	no_of_same_packet	Integer	Fuzzy
7	Same_source	yes – no	Boolean
8	Same_dest	yes – no	Boolean
9	Average_packet_size	Integer	Fuzzy
10	Window_size	Integer	Fuzzy
11	No_of_packets	Integer	Fuzzy
12	Last_packet_flag	Char	Crisp
13	First_packet_flag	Char	Crisp
14	System	Char	Crisp
15	TTL	Integer	Fuzzy
16	Data_transfered	integer (sent data + received data)	Fuzzy
17	Header_size	Integer	Fuzzy
18	Same_day	Boolean (1 if same day)	Boolean
19	Is_working_time	Boolean (1 if working time)	Boolean
20	Is_broadcast	Boolean (1 if destination is broadcast)	Boolean
21	Timestamp	Time (connection time)	Fuzzy
22	Source_ip	IP format	Crisp
23	Destination_ip	IP format	Crisp

4.3.3 Network Attacks

Security experts have classified computer and network attacks into four different types, this is also consonant with the KDD'99 dataset classification. The four attacks classes are:

1. Denial of Service (DoS): Excessive consumption of resources that denies legitimate requests from legal users on the system. Nowadays there are new version of DOS which called Distributed Denial of Service (DDOS) which is the basically same as DOS but the overwhelmed requested comes from different sources not only one as in DOS. One of known attacks in this category is the Apache2 attack which is a denial of service process tend to attack the web server process by flooding it, in this attack an attacker sends a request with many http headers, this will end up slowing down server or crash it [199].
2. Probes or Scanning: Attacks that can automatically scan a network of computers to gather information or find known vulnerabilities. Probe is a reconnaissance attack designed to uncover information about the network and used to gather information from the systems of victim. Example of this type is IPSweep attack which is a surveillance sweep to determine which hosts are listening on a network to know which hosts are working and to gather vulnerabilities if any [199].
1. Remote to Local (R2L): Attacker having no account gains a legal user account on the victim machine by sending packets over the networks. Example of this type is the well-known attack called Dictionary or Dict for short, here an attacker tries to gain access to some machine by making repeated guesses at possible usernames and passwords [199, 200].
2. User to Root (U2R): User to Root attacks are belong to the class of attacks where the attacker gains access to a normal user account on

the system and by exploiting some vulnerabilities obtains the root access. The most common User to Root attack is buffer overflow attack, which enables the attacker to run personal code on a compromised machine once the boundary of a buffer has been exceeded, giving him/her the privileges of the overflowed program which in most cases is root [199].

For the purpose of this study other types of attacks was considered like session hijack attacks, web applications attacks and data attacks. Appendix A shows detailed information about the attacks used on this study and the rules extracted from those attacks.

Table 4.5 below shows the whole list of 144 attacks studied carefully for the purpose of filling the knowledge base with real information reflecting the general behaviour of those attacks.

Table 4.5. Attacks used in extracting rules and in tests

Group Type	Attacks Studied	Attacks
Denial of Service (DoS)	Apache2, Smurf, Neptune, DOSnuke, Land, POD, Back, Teardrop, TCPreset, Syslogd, CrashIIS, ARPPoison, Mailbomb, Selfping, Processtable, UDPstorm, http GET flooding attack, SSHprocesstable, WinFreez, Fraggle DoS Attack, Ping-Pong, Loki, DHCP starvation attack,Mac Flooding, Newtear, Bonk, Boink, Trin00 (Win Trinoo), Tribe Flood Netowrk (TFN), Shaft, Stacheldraht, Mstream, TFN2K, Knight, Trinity, UDP Flood attack, DNS Query attack, Back slash, DRDoS attacks, CGI request attack, ARP storm attack, Algorithmic complexity attack, Spam Attack	44
Probes	Portsweep, IPsweep, Queso, Satan, MSscan, NTinfoscan, Lsdomain, Illegal-sniffer, Saint, Resetscan, Nmap, Xmax scan, Fin Scan, Port Scan, Ping Sweep, Stealth Scan, Null Scan, Idle Scan, ICMP Echo Scan, List Scan, UDP Scanning, Syn/Fin Scanning, Inverse TCP Flag Scanning, Ack Flag Scanning, Nessus, Https sniffing through fake SSL certificate, HTTPS sniffing through sslstriping	27
Remote to Local (R2L)	Dictionary, Netcat, Sendmail, Imap, Ncftp, Xlock, Xsnoop, SSHtrojan, FrameSpoofer, Ppmacro, Guest, Netbus, SnmpGet attack, Ftpwrite, HttpTunnel, Phf, WarezClient, Spy, SNMP Guess attack, Named, Guess Password, Multihop, WarezMaster, GuessPOP, GuessFTP, GuessTelnet, WORM	28
User to Root (U2R)	Sechole, Xterm, Eject, Ps, Anypw or Nukepw, Perl, Yaga, Fdformat, Ffbconfig, Casesen, Ntfsdos, Loadmodule, Sqlattack, Rootkit, Buffer_overflow	15
Session Hijack Attacks	Brute Force, HTTP referrer attack, Cross-site script, Session fixation, TCP/IP hijacking, RST hijacking, Blind hijacking, UDP hijacking	8

Web Applications Attacks	HTTP response splitting attack, Web cache poisoning attack, HTTP bruteforce attack, Unvalidated input, Parameter/form tampering, SQL Injection, Command injection, File injection attack, XSS Attack, Cookie poisoning attack	10
Other Attacks	Secret, DHCP Starvation Attack, Rogue DHCP server attack, ARP spoofing, MAC spoofing, DNS poisoning, Web spoofing, Fragmentation attack, TTL attack Tiny fragment attack, Steganography, Mitnik attack, cross-site request forgery	12
Total		**144**

In this research normal behaviour has been carefully studied as well, and therefore tens of rules belongs to normal profiles group was extracted, examples are shown in Table 4.6 below.

Table 4.6. Rules extracted from Normal traffic

Profile Name	**Extracted Rules**
Normal Telnet	logged_in = 1 AND protocol_type = tcp AND service = Telnet AND flag = SF AND src_bytes = many AND dest_bytes = xmany AND same_srv_rate = many
Normal http	logged_in = 1 AND protocol_type = tcp AND service = http AND flag = SF AND (src_bytes = few OR average) AND dst_bytes = average AND dst_host_count = few AND dst_host_srv_count = few AND same_srv_rate = many AND dst_host_same_srv_rate = many
Normal smtp	logged_in = 1 AND protocol_type = tcp AND service = smtp AND flag = SF AND src_bytes = xmany AND dest_bytes = few AND dst_host_count = average AND dst_host_srv_count = many AND same_srv_rate = many AND dst_host_same_srv_rate = xmany
Normal FTP	logged_in = 1 AND protocol_type = tcp AND (service = ftp OR ftp_data) AND flag = SF AND dst_bytes = average AND dst_host_count = few AND dst_host_srv_count = few AND same_srv_rate = many AND dst_host_same_srv_rate = many AND hot > = 4
Authentication	logged_in = 1 AND protocol_type = tcp AND service = auth AND flag = SF AND dst_bytes = vfew AND

	src_bytes = vfew dst_host_count = few AND dst_host_srv_count = few AND same_srv_rate = many AND dst_host_same_srv_rate = many
NTP	protocol_type = udp AND service = ntcp_u AND flag = SF AND dst_bytes = vfew AND src_bytes = vfew dst_host_count = few AND dst_host_srv_count = few AND same_srv_rate = many AND dst_host_same_srv_rate = many
ICMP Echo reply (1)	protocol_type = ICMP AND service = ecr_i AND flag = SF AND duration = short AND dst_bytes = vfew AND src_bytes = vfew AND dst_host_count = few AND dst_host_srv_count = few AND same_srv_rate = many AND dst_host_same_srv_rate = many AND dst_host_same_src_port_rate = many

4.4 Adaptive Component

Innate immune system originally programmed defence mechanism, and uses general characteristics to detect invaders, is actually not enough to protect the body from microbes that are able to evolve rapidly to overcome innate protection. Adaptive immunity allows for the body to adaptively detect and destroy invading specific pathogens.

In this thesis, a typical adaptive immune system structure is being adopted which is widely been applied, for instance in [56, 116, 201] and described in details in [13]. To be able to apply intrusion detection capability based on adaptive immune system framework at least three steps should be followed; the first step is to use reasonable representation for the elements in the network and their interactions, for example, antigen is used in AIS to show the abnormal activity in IDS. Then generating chosen algorithms as appropriate and the third step is to optimize those algorithms [113].

In our proposed framework, the adaptive component is simulating the adaptive immune response to antigen stimulus. It is basically consisting of

three main algorithms, i.e. artificial immune network theory, negative selection algorithm and clonal selection algorithm.

The immune network theory is aimed to maintain stability of the system by interconnecting network of cells. In this theory, two populations are made up the B-cell population, which are the initial population generated from raw training data and the cloned population which is used for antigen training. The negative selection algorithm is the process of protecting the immune system from reacting to its own cells, while the clonal section algorithm is the process aimed of ensuring that only cells able to recognize foreign invaders will proliferate and cloned, it is also ensuring diverse type of detectors for better coverage.

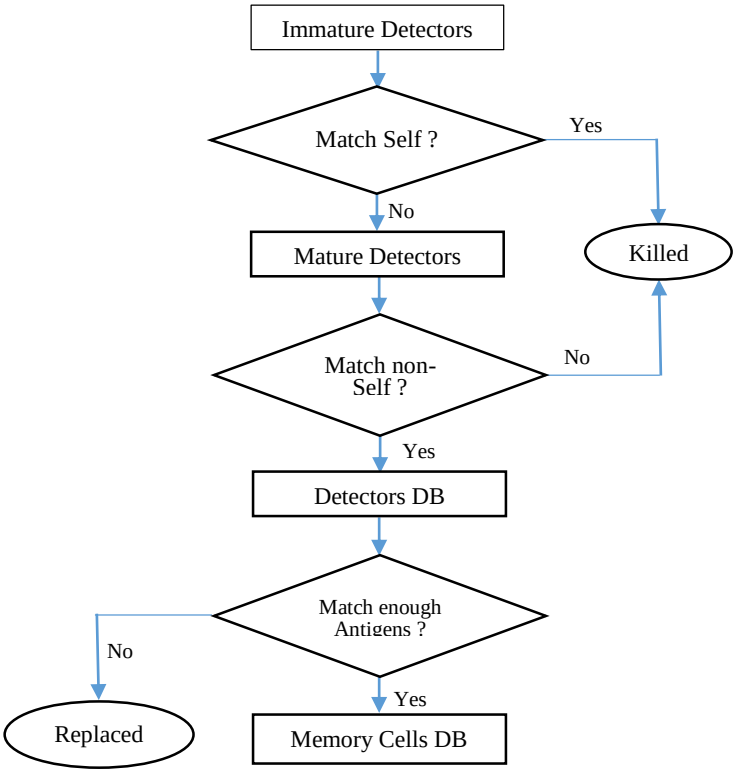


Figure 4.6. Detectors generation process [19]

Figure 4.6 describes detectors generation process and maintaining their diversity and distribution before eliminating unwanted detector cells and keeping memory cells for the future attacks. Immature detectors sets will be chosen through random selection, these immature detectors pass

through negative selection algorithm, if the detector matches self-sets, it will be discarded and otherwise it will be added to a mature detectors database.

Figure 4.7., explaining the life cycle of the detectors as proposed by Hofmeyr and Forrest [202] and followed by the research with some differences in the thresholds, co-stimulation and matching algorithms.

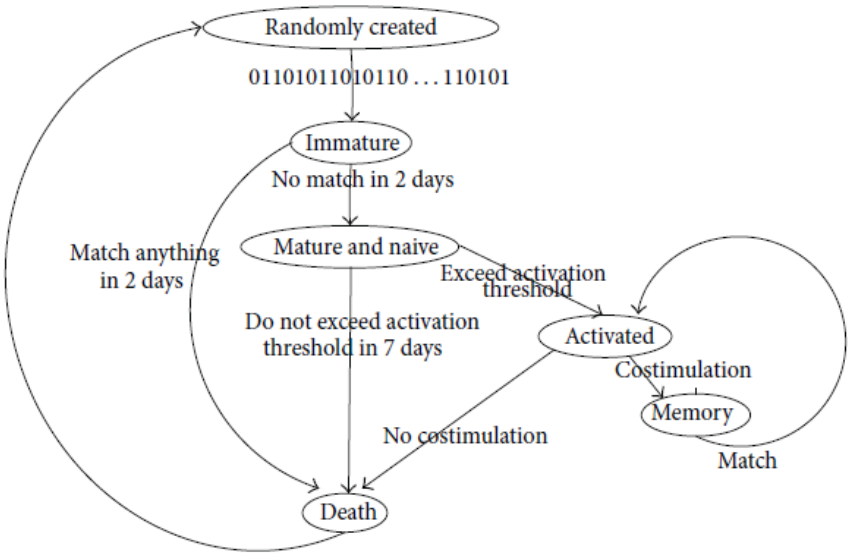


Figure 4.7. Detectors life cycle process [202]

The antigen and antibody sets are constructed as fixed length binary strings extracted from the Internet Protocol packet in a network environment and consist of main attributes like port number, protocol type, flags, packet length, etc. Self and non-self- sets are collected from normal and abnormal network traffic respectively during training. The length of these string sets are subject to more research since long sets produce more accurate results but needed bigger resources [13, 54, 56].

These mature detectors sets will be entered into clonal selection algorithm, in which they will be compared with non-self-sets, if they match with high affinity they will clone themselves and produce new sets with minor changes. If mature detector matches with enough antigens in a certain period of time then it will be added to memory detectors which have smaller threshold value and longer life cycle, if not, this detector will be

subject to replacement soon. To calculate the affinity in negative selection and clonal selection algorithms hamming distance affinity string used which efficiently calculates bit differences between two binary strings. Traffic passes from innate layer will be compared to detectors generated from the above process, match traffic will be blocked and copy of these data will be used to help produce more non-self-sets in a training unit, others will be passed directly to the network.

4.4.1 Detectors Representation

As mentioned above the self-cells and non-self-cells are defined as the normal and abnormal TCP/IP connection among the computers, the collection is characterized by the main TCP/IP Connection attributes such as source IP, destination IP, services, etc. Table 4.7 shows mapping relationship between adaptive immune system and proposed security framework. Antigens and Antibodies or detectors are represented as fixed length binary strings. Since data are eventually implemented as binary bits in computers, researches are normally focused on binary representation as mainstream.

Table 4.7. Mapping relationship between BIS and security defence system

Organism	Network
Pathogen (Antigen)	Intrusions or Viruses
Antibody – Antigen	Binary String
Antigen/Antibody Binding	Matching Algorithm (Pattern Matching)

16-B string has become the de-facto antivirus industry standard for signature based IDS, researchers at IBM have shown that 16B is sufficient to identify malicious code with a proximately 0.5% false positive rate [13]. In this framework 256 bit binary string size is used, this guarantees more accurate information since the system is working offline and about 80% of the traffic already dealt with by the first component, the innate layer. The LISYS which is designed as a light weight detection system compressed in a set of 49-bit string format mainly for TCP SYN packet [78]. Later Harmer and the team [13] extended LYSIS further and used

320-bit binary string for each antibody signature, comprising 29 of the possible data fields in a network protocol packet, for TCP, UDP and ICMP [80].

The 256 bit binary string for representing the antibodies are segregated to utilize the IP packet structure as a template. Only the most common three protocol types TCP, UDP and ICMP are used for the purpose of this research. Table 4.8 below shows the main fields mapped to the 256 bit binary string.

Table 4.8. Mapping main fields to the 256 bit binary string relationship

No	Field	Number of bits	Possible values
1	Protocol Type	2	TCP, UDP or ICMP (1,2,3)
2	Time To Live (TTL)	8	Usually less or equals 128
3	IP Flags	16	0-65535
4	Packet Length	16	0-65535
5	IP Source Address	8	0-255
6	IP Destination Address	8	0-255
7	IP identification Number	16	0-65535
8	Source Bytes	16	0-65535
9	Destination Bytes	16	0-65535
10	TCP Source Port	16	0-65535
11	TCP Destination port	16	0-65535
12	TCP Sequence Number	32	Any
13	TCP Acknowledge Number	32	Any
14	TCP Flags	8	0-255
15	TCP Packet Size	16	0-65535
16	UDP Source Port	16	0-65535
17	UDP Destination Port	16	0-65535
18	UPD Packet length	16	0-65535
19	ICMP Source Port	8	0-255
20	ICMP Destination Port	8	0-255

4.4.2 Matching Algorithm

The affinity between antibody and antigen is decided by using different matching techniques. Several algorithms have been frequently used to determine the affinity, such as Eucliden distance algorithm, Hamming distance algorithm, r-chunk algorithm and r-contiguous bit rule algorithm [117, 203].

In the applied adaptive layer only the receptor region on the surface of a lymphocyte is represented which is the region that binds to foreign invaders in a process called recognition. The detection or recognition process or binding is represented as string matching and detection of a

string occurs when there is a match according to a matching rule. String matching is used here because it is simple and efficient and easy to analyse and implement.

The matching of two strings is determined by a function that produces a binary output either match or not-match according to predetermined rules. Generally, binary representation is general enough to consider as an idle representation for any type of data, since any computer data regardless of its type is represented as a sequence of bits in the memory of a computer [14].

A binary matching rule is a rule that is defined in terms of individual bit matching of detectors and antigens represented as binary strings. The following paragraphs give some ideas on the main types of binary string matching algorithms:

r-contiguous Matching Algorithm:

A random detectors are generated before tested for matching with self and non-self sets. A detector string was said to match an antigen string if the two strings identically shared the same characters in an uninterrupted stretch of *r* bits [14, 56, 119].

The binary matching process is defined as follows: given $x = x1x2 \ldots . . xn$ and detector $d = d1d2 \ldots \ldots dn$,

$$d \text{ matches } x \equiv \exists i \leq n - r + 1 \text{ such that } x_j = d_j \text{ for } j = i, \ldots, i + r - 1,$$

r-chunk Matching Algorithm

This matching rule subsumes r-contiguous matching, that is, any *r*-contiguous detector can be represented as a set of *r*-chunk detectors [14]. The *r*–chunk matching rule is defined as follows: given a string $x = x1x2 \ldots . xn$ and a detector $d = (i, d1d2 \ldots . dm)$, with $m \leq n$ and $i \leq n - m + 1$,

$$d \text{ matches } x \equiv \ x_j = d_j \text{ for } j = i, \ldots, i + m - 1,$$

where i represents the position where the r -chunk starts. Some preliminary experiments suggest that the r-chunk matching rule can improve the accuracy and performance of the negative selection algorithm [14].

Hamming Distance Matching Algorithm:

The hamming distance is the most commonly used method for measuring the distance between bit strings, although several researchers proposed additional measures that extend the hamming distance. The hamming distance taking the complement results in the number of bit positions that are alike:

$$\text{Hamming similarity} = \sum_{i=1}^{N} \overline{(X_i \oplus Y_i)}, \quad X, Y \in \{0,1\}^N.$$

given a binary string $x = x1x2 \ldots xn$ and a detector $d = d1d2 \ldots dn$,

$$d \text{ matches } x \equiv \sum_{i} \overline{x_i \oplus d_i} \geq r,$$

Where $\oplus$ is the exclusive -or operator, and $0 \leq r \leq n$ is a threshold value.

Euclidean Distance Algorithm:

In the euclidean distance $d(x, y)$ the two vectors $x = \{x1, \ldots\ldots, xn\}$ and $\{y = y1, \ldots\ldots, yn\}$ from n-dimentional space. So the euclidean distance between x and y can be calculated as:

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + \ldots + (x_n - y_n)^2}, \quad d(x,y) \in \langle 0, \infty)$$

4.4.3 Co-stimulation Signal

In biology co-stimulation or second signal is aimed to prevent immune cells from incorrectly reacting against self-cells, so the purpose is to minimize the false alarm by redetecting harm invaders. The active detectors receive two signals telling them that they bound to pathogens not to self-cell.

In the security framework proposed, co-stimulation layer was added for rechecking both normal and abnormal traffic and feed the system back

with the results, this will help the system react in better way to the same attack and normal connections. In experiments, results of co-stimulation layer compared with other results gained before and adding this layer are given.

4.5 Conclusion

In this chapter, the multilayer AIS framework for network defence is introduced. The innate layer of the framework was performed using a fuzzy expert system algorithm. It has also been shown how to construct the fuzzy expert system using examples. The network data is performed using typical KDD'99 dataset with improvements to overcome some of its negative effects. The adaptive layer has been explained to also use a typical algorithm constructed of combining three algorithms.

This chapter constitutes the main contribution of this thesis i.e. the multilayer framework and the innate layer algorithm.

CHAPTER 5

EXPERIMENTS

5. Experiments

5.1 Experimental Setup

As illustrated in Figure 5.1, nine Windows based operating system machines were used to test the system, all with duo processor 2.5 GHz, 500 GB hard disk and 8 GB of RAM, these computers are connected in a separate LAN network using 16 ports switch. Machines (1) and (2) are used as an Input Unit in which network traffic in different formats prepared to be entered into innate layer and some features will be extracted here as well, the Input Unit roles are described in details in chapter 4.

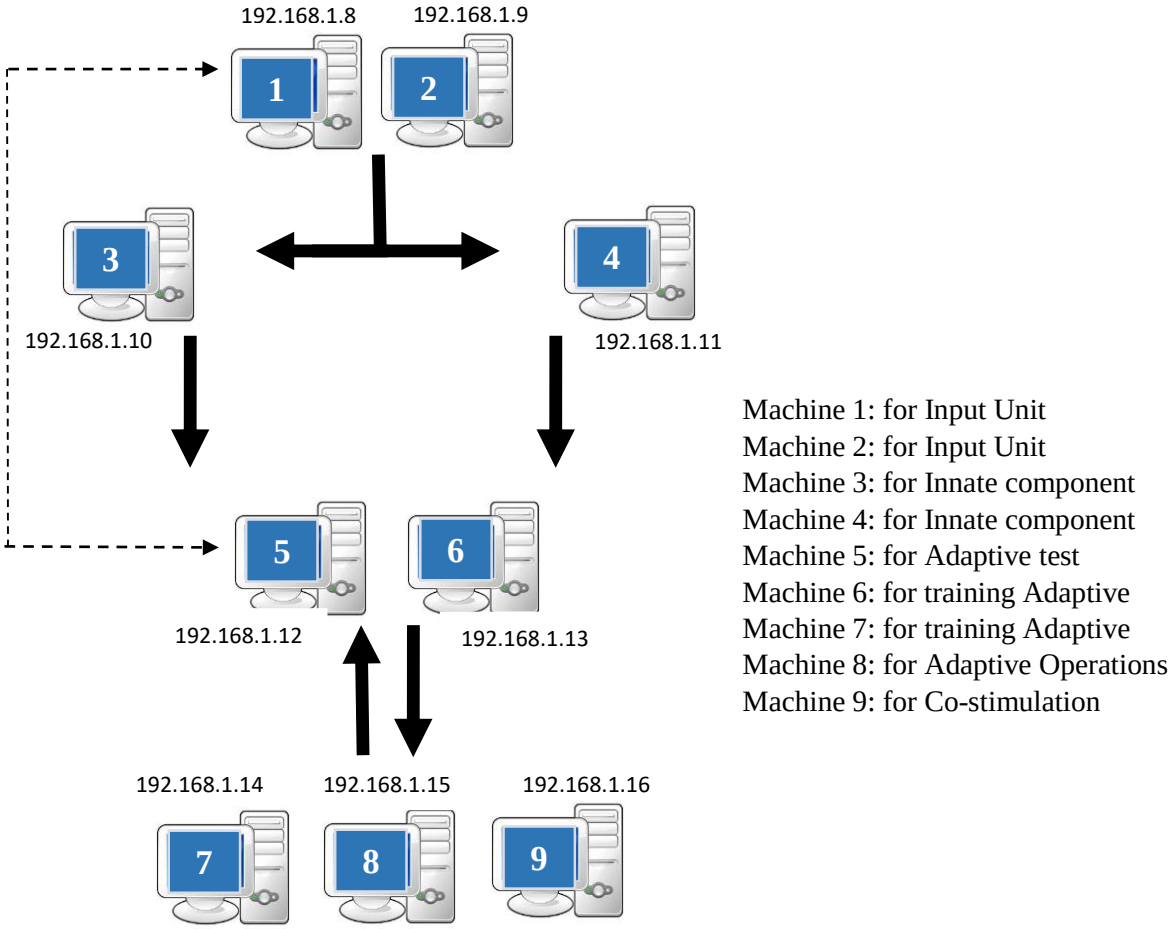


Figure 5.1. Network configuration used in experiments

Machines (3) and (4) were used for innate immune component including the test operations using KDD'99 and NSL-KDD datasets as initial input. Machine (5) is being used for testing adaptive immune component while Machine (6) and (7) are for constructing detectors and they are prepared

to perform training tasks to self and non-self-sets too. Machine (8) is used to match antigens and antibodies while Machine (9) is used for co-stimulation.

Four software programs are developed using PHP and installed in different PCs for input unit, innate component, adaptive component and co-stimulation component.

The test setup is designed to mimicking the real immune system response where different components are distributed, parallel and connected without central control.

It is vital to reveal that several informal tests conducted before performing the formal tests, the results for those initial tests being used to make the defence system more effective by enhancing the overall performance.

In a period of four weeks three tests were conducted; two for the innate immune layer using corrected KDD'99 dataset with 3000 new connections generated and added to represent new attacks, the third test is for the adaptive layer alone using innate output traffic. The last test performed in a period of two weeks for the adaptive layer after adding co-stimulation signal, human modifications are presented in the co-stimulation test to better understand the gaps for the purpose of enhancing the overall performance of the system just as the biological second signal doing in nature.

KDD'99 is proved to be a practical in terms of evaluating the performance of intrusion detection systems in hundreds of research papers. It is also vital to mention that DARPA evaluation dataset is used for the purpose of training as well not only testing. In a period of six months of training time, random records selected from KDD'99, 10% KDD dataset and corrected KDD dataset as the 10% KDD dataset in a daily basis.

As mentioned in chapter 4, the corrected KDD'99 dataset is more balanced compared to the original KDD'99 dataset and to the 10% KDD dataset

and has bigger number of attacks which are 37 attacks classified in four groups: Denial of Service (DoS), Probes (Scanning), Remote to Local (R2L) and User to Root (U2R). The number of attacks connections in the corrected KDD dataset are 250436 while the number of the normal connections are 60593. To have more balanced traffic and to reduce the memory usage in the test only 500 connections or less were tested for each attack and 8000 connections from normal connections then 3000 more connections and 3000 constructed connections from new attacks were added, those sample connections are randomly selected after the input unit eliminate duplicated traffic, so 13655 attacks connections and 8000 normal connections were tested.

Table 5.1 shows the number of attacks and normal connections for the test instances of the KDD'99, corrected and 10% datasets.

Table 5.1. Test dataset for KDD'99

Dataset	DoS	Probes	U2R	R2L	All Attacks	Normal	Attacks
10% KDD'99	391458	4107	52	1126	396743	97277	24
Corrected KDD'99	229853	4166	70	16347	250436	60593	37
Whole KDD'99	3883370	41102	52	1126	3925650	972780	39

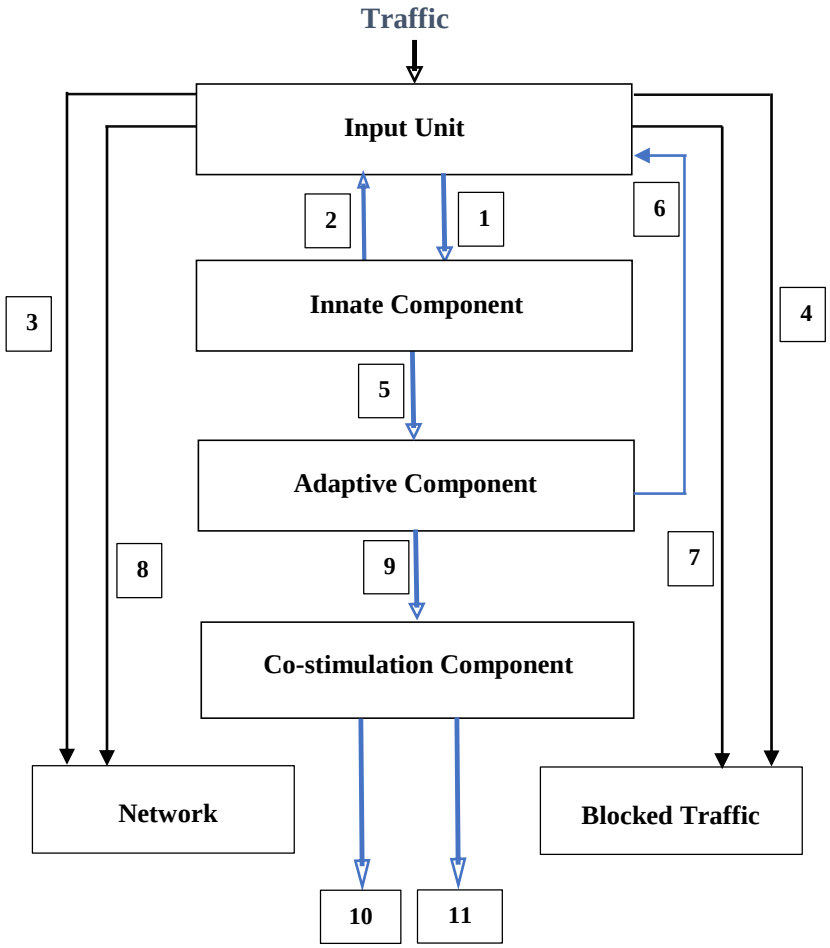
To further validate and benchmark obtained results, extra three tests were conducted using NSL-KDD dataset. NSL-KDD is a refined version of KDD'99 dataset, it is relatively new one suggested to solve some of the inherent problems of the KDD'99 dataset, although it is still not yet considered a public dataset for network-based IDSs and may not be a perfect representative of real networks, but it is quite good dataset for benchmarking and comparing different methodologies [204].

Table 5.2. Test dataset for NSL-KDD

Dataset	DoS	Probes	U2R	R2L	Normal	All	Attacks #
NSL-KDD (Test Dataset)	7456	2421	200	2756	9711	22544	37

The NSL-KDD dataset has managed to solve two main issues in the KDD'99 dataset, i.e. it has no redundant records in the train set and no

duplicate records in the test set and it has sufficient number of connections for train and test datasets. The test sets just like in KDD'99 has 37 attacks grouped into the same four categories: DoS, Probe, U2R and R2L [205]. Table 5.2 shows number of different record numbers in the test instances of the NSL-KDD dataset [204].



0- Input traffic entered into Input Unit
1- Lookup table sent to Innate component containing all necessary information
2- Lookup table showing connections to block or ignore or send to adaptive
3- Real traffic sent to Network according to Innate component check
4- Real traffic blocked according to Innate component check
5- Lookup table sent indicating traffic need to be check by Adaptive component
6- Lookup table sent showing which connections to block or to send to network
7- Real traffic sent to Network according to Adaptive component check
8- Real traffic blocked according to Adaptive component check
9- Lookup table sent to co-stimulation for second check
10- New normal list after second check
11- New abnormal list after second check

Figure 5.2. Traffic flow for the proposed framework

Figure 5.2 shows the flow of the traffic as described in details in chapter 4, the network setup and software beside tests conducted are all accomplished taking into account the flow of traffic and the functions of each component specially the central role of the Input Unit.

5.2 Tests Software

Four software programs used to train and test the proposed multilayer AIS defence system, those four programs are installed in different machines but still they are connecting among each other as required.

The first program is for Input Unit and this is the central software and acting the role of the communicator, it is programed for the purpose of preparing traffic for the main components of the framework, i.e. innate and adaptive components. The software is also programed to prepare a lookup table containing connection number and time stamp, it is connected to innate and adaptive programs for the purpose of responding to their instructions regarding blocking or sending payload data.

The second program is for innate component which is the main component of our thesis since it is simulating and testing the innate immune system functionality. This software is used to program fuzzy logic system different components including the construction of the fuzzy sets, inference engine, fuzzification and diffuzification processes. Figures 5.3 and 5.4 show screenshots from the fuzzy logic software, the first figure is showing the knowledge base with some entries while the second figure shows the tab responsible for all settings related to fuzzy sets construction.

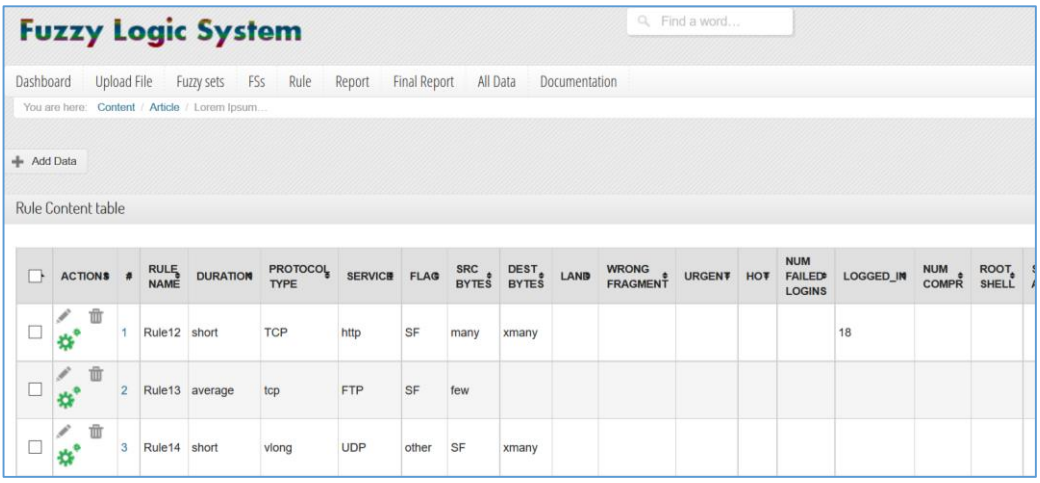


Figure 5.3. Screenshot from fuzzy logic software – knowledge base

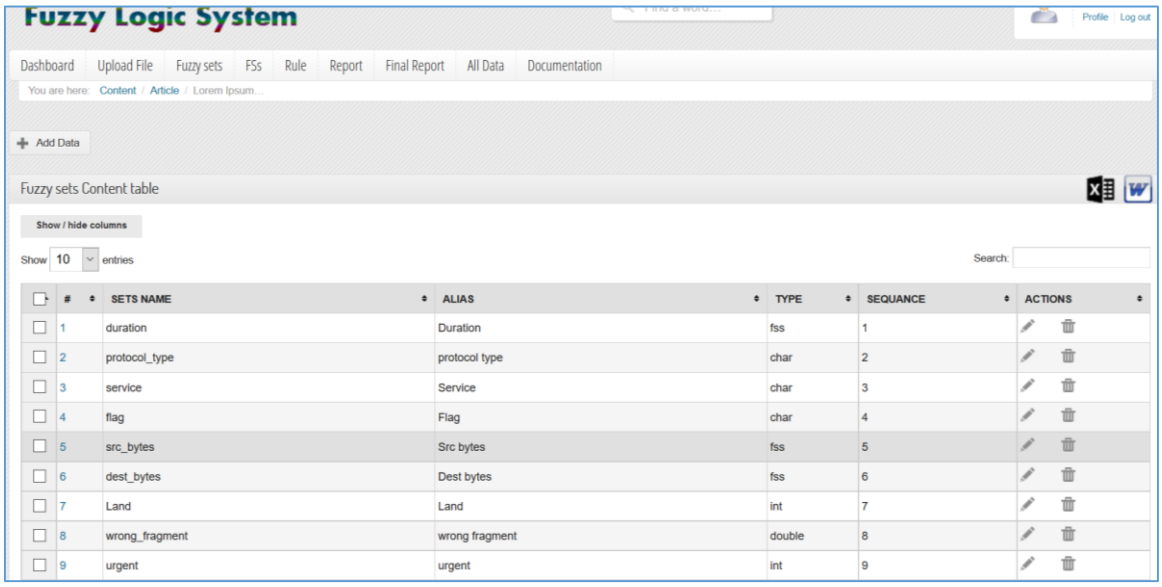


Figure 5.4. Screenshot from fuzzy logic software – fuzzy sets construction

The remaining two programs are for the adaptive immune system component. The first software is programed to perform all for adaptive layer processes and algorithms including training the detectors, matching algorithms, controlling detectors diversity, keeping memory detectors, etc., beside training self and non-self-sets. The last software is for testing the adaptive immune component before and after co-stimulation process.

5.3 Experiments Results

The first test was applied to the innate component by entering connections from the 37 attacks in the corrected KDD dataset; the detailed results are illustrated in Table 5.3 below. Although the innate system concerns only about general characteristics of the connection and is not responding

specifically to attack but still this test conducted compare the detection abilities of the system for each individual attack so to help on better enhance the whole detection mechanism in the future.

Table 5.3. Result of the first innate component test

No	Attack Name	Corrected Dataset	Samples	Detected Instances	TP Rate%
1	Apache2	794	500	420	84.00
2	Back	1098	500	401	80.20
3	Buffer_overflow	22	22	10	45.45
4	Ftp_write	3	3	1	33.33
5	Guess_password	4367	500	405	81.00
6	Httptunnel	158	158	104	65.82
7	Imap	1	1	1	100
8	IPsweep	306	306	245	80.06
9	Land	9	9	5	55.55
10	Loadmodule	2	2	1	50.00
11	Mailbomb	5000	500	434	86.80
12	Mscan	1053	500	419	83.80
13	Multihop	18	18	11	61.11
14	Named	17	17	9	52.94
15	Neptune	58001	500	426	85.20
16	Nmap	84	84	66	78.57
17	Perl	2	2	1	50.00
18	Phf	2	2	1	50.00
19	Pod	87	87	45	51.72
20	Portsweep	354	354	256	72.31
21	Processtable	759	500	410	82.00
22	Ps	16	16	8	50.00
23	Rootkit	13	13	7	53.84
24	Saint	736	500	412	82.40
25	Satan	1633	500	369	73.80
26	Sendmail	17	17	10	58.82
27	Smurf	164091	500	412	82.40
28	Snmpget	7741	500	401	80.20
29	Snmpguess	2406	500	390	78.00
30	Sqlattack	2	2	2	100
31	Teardrop	12	12	7	58.33
32	Udpstorm	2	2	2	100
33	Warezmaster	1602	500	380	76.00
34	Worm	2	2	1	50.00
35	Xlock	9	9	6	66.66
36	Xsnoop	4	4	3	75.00
37	Xterm	13	13	6	46.15
Attacks Connections		**250436**	**7655**	**6087**	**79.52%**
Normal Connections		**60593**	**8000**	**6205**	**77.56% (TNR)**
All Connections		**311029**	**15566**	**12292**	**78.54%**

To guarantee realistic results the behaviour of 144 attacks including KDD attacks were carefully studied as shown in details in chapter 4, then tens of rules added to the knowledge base extracted from attacks behaviours.

The second test conducted is including 3000 connections constructed in Sudan-CERT labs, the majority of these connections are new attacks. Then randomly 3000 attacks connections added from KDD dataset to have more realistic traffic.

Results of the innate layer for both KDD dataset and added samples are shown in Table 5.4, the results showed that the system can deal with more than 79% of the connections, as the system being able to deal with more traffic this will help reduce the amount of storage and processing needed for the adaptive layer. During the system setup an investigation has been generated to different possible amount of traffic can be handled by adaptive immune component in the proposed system, it is found that the exact critical point in which the adaptive layer will start falling to respond effectively if reached is 31% of the whole traffic.

Six performance evaluation metrics are calculated in all tests conducted:

1. True Positive Rate (TPR): the percentage of anomaly traffic correctly classified as anomalies.
2. False Negative Rate (FNR): the percentage of anomaly traffic wrongly classified as legitimate.
3. False Positive Rate (FPR): the percentage of legitimate traffic wrongly classified as anomalies.
4. True Negative Rate (TNR): the percentage of legitimate traffic correctly classified as not an anomaly or threat.
5. Accuracy Rate: is the measurement of the number of correctly classified instances. It is calculated as follow:

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

6. Detection Rate (DR): is the correctly detected attacks compared to the total number of attacks:

$$DR = \frac{TP}{TP + FN}$$

As shown in table 5.4 the innate component reached a true positive and true negative rates of 76.56% and 77.56% respectively, the results also show that the average false positive rate is 0.017 while the total false negative rate is only 0.007. The tested system achieved accuracy rate equals to 98.44% and detection rate equals to 97.79%.

Those results are quite good taking into account the fact that there is still one more layer of defence for unknown traffic using totally different mechanism. Even better results can be achieved when correcting errors and adding more rules to the fuzzy knowledge base.

It is vital to emphasise that a false negative rate is the most serious and dangerous since the system accepted traffic as legitimate but it actually an attack, here in this situation the administrators and security professionals do not know an attack is exist. False positive also can cause significant issues specially when there are real overhead to the network.

Table 5.4. Results of the Innate Component

Data Types	KDD Corrected		Sent to Adaptive		TPR	FPR	FNR	TNR
	All	Tested	#	%	%	%	%	%
Normal	60593	8000	1656	20.70 %	76.56 %	0.017	0.00734	77.56 %
Attacks	250436	10655	2812	20.59 %				
Added Attacks	3000							
All	**314029**	**21655**	**4468**	**20.63 %**	**76.56 %**	**1.7 %**	**0.73 %**	**77.56 %**

The third conducted test is for the adaptive component alone, the input for this test is the connections considered as unknown from the innate layer test. Detectors, self-sets and non-self-sets are collected and constructed during six months training period.

As shown in Table 5.5 below, about 88.7% of the traffic passed from the innate layer has been correctly classified as being attack or normal connection, the initial results show an average of 6.78% false positive rate and average of 3.58% false negative rate, these error rates could be enhanced automatically when more traffic being trained. The test also shows an accuracy rate of about 94% and detection rate is about 96%.

Table 5.5. Results of the adaptive component

	Connections	Detected	TP Rate	TN Rate	FP Rate	FN Rate
Attacks passed from innate	2812	2601	92.49 %	84.96 %	6.78 %	3.58 %
Normal traffic passed from innate	1656	1407				
Accuracy Rate = 94.48% Detection Rate = 96.27%						

As stated above, yet one more test were conducted for the adaptive layer after co-stimulation process. The objective of this test is to reassess the adaptive layer alone when adding co-stimulation signal as another check point, the co-stimulation component rechecks correctness of the detection of the connections after adaptive immune component classification, so it is the main role is to check weather adaptive filtration is correct. The results after adding this check show remarkable improvement as shown in Table 5.6 below.

Table 5.6. Results of the adaptive layer test after co-stimulation

TP Rate	FP Rate	FN Rate	TN Rate
96.675 %	0.78 %	0.89 %	94.23 %
Accuracy Rate = 99.13% Detection Rate = 99.08 %			

Figure 5.5 shows the results of the main components of the system, the innate and adaptive components including the test with the addition of co-stimulation signal. The results including the six metrics mentioned earlier for performance evaluation.

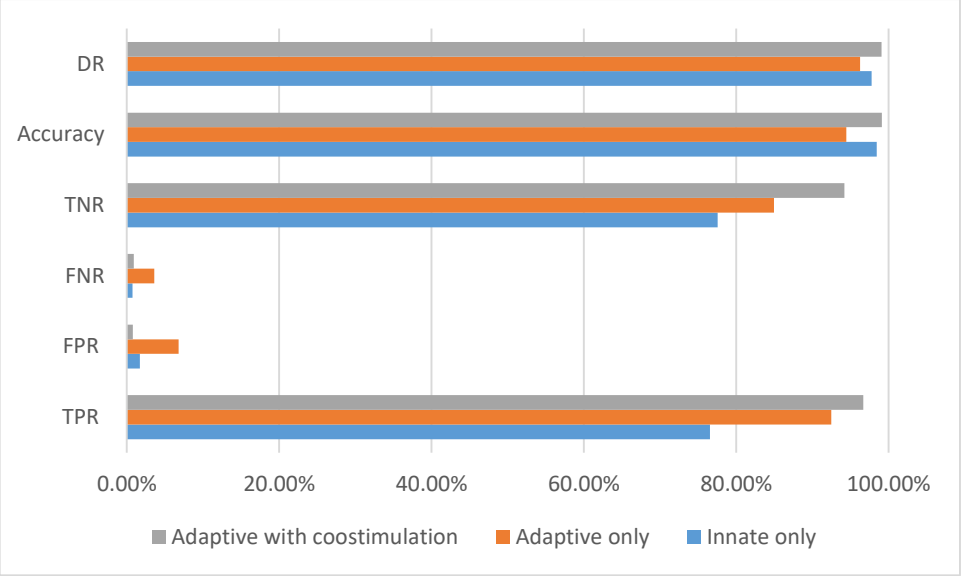


Figure 5.5. Test results for different components

For the purpose of benchmarking and validating the results obtained earlier it is being decided to conduct three more test using NSL-KDD dataset, the tests are for the innate component, adaptive component and adaptive component after co-stimulation check.

The results of those three tests are in Table 5.7 and are reflected in Figure 5.6 as well, all test instances available in the NSL-KDD dataset were used without extracting any samples, so the test instances were 22544 record. The results are looking the same for the innate component while they are lower in adaptive component, this is because the system has not being trained with the NSL-KDD training dataset. It is important to mention that as results earlier suggested, around 20% of the traffic from the innate component are classified as unknown and passed to the adaptive component, so results of the innate component in Table 5.7 are for the rest of the records not including the traffic passed to the adaptive layer.

Table 5.7. Test results using NSL-KDD

Test Conducted	TPR	FPR	FNR	TNR	Accuracy	DR
Innate only	91.76%	1.67%	0.64%	94.33%	98.77%	99.30%
Adaptive only	89.22%	7.41%	3.58%	84.21%	94.04%	96.14%
Adaptive with co-stimulation	93.39%	0.78%	1.27%	92.13%	98.90%	98.65%

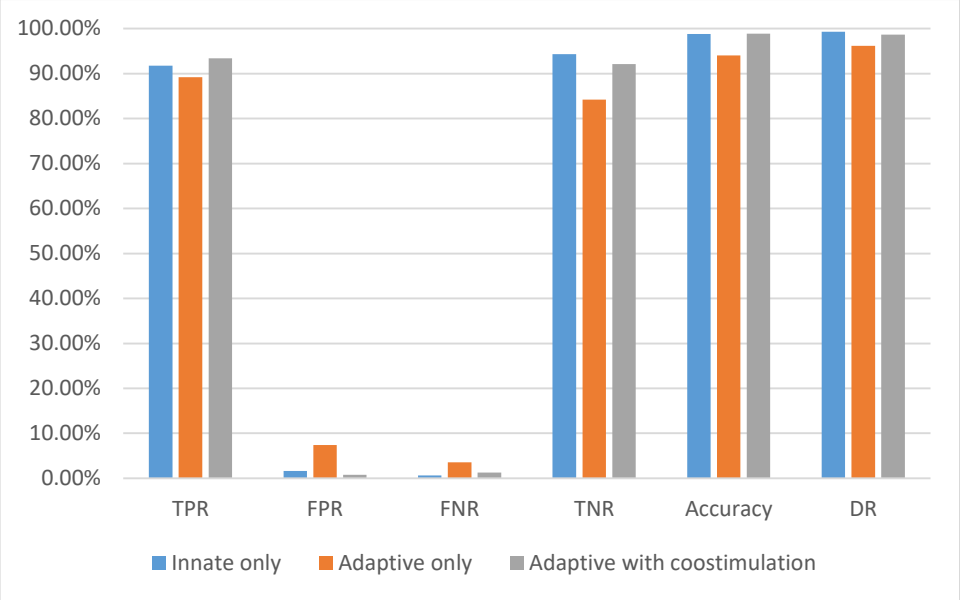


Figure 5.6. Test results using NSL-KDD

Comparing results obtained for the whole system to recently conducted tests in the field of IDS, we are witnessing a very encouraging research especially the results of the innate layer alone and the adaptive layer results after adding co-stimulation layer. And for sure one of the contributions of the proposed system which have been noticed during tests, its great abilities to detect new attacks not only signature based attacks.

Results obtained are very good comparing to most of the results in Ernst et al. [206] survey, in which writers evaluated different types of approaches of intrusion detection systems and showed examples and results for chosen researches, the approaches reviewed included specification method approach, Support Vector Machines, machine learning approaches, behaviour-based approaches, mobile agents approach, genetic network programming, fast inductive learning, situational awareness, back propagation and fuzzy logic approach.

Shah and Isaac [207] provided a comparison study of the performance of two well-known open source intrusion detection systems, which are Snort and Suricata. Both IDSs triggered a high rate of false positive alarms. Snort triggered 55.2% FPR compared to Suricata's 74.3% FPR. Snort had

a high detection accuracy and triggered only 6.7% FNR whereas Suricata triggered 16.7% FNR while processing the same malicious traffic.

In [208] writer proposed an approach for detecting anomalies in mobile adhoc network based on genetic algorithm and artificial immune system, called GAAIS. This approach evaluated by comparing it with two other dynamic approaches, DCAD and WPCA. Experiment results showed that the average detection rate of GAAIS is 95.44% with average false alarm of 3.59% which are proof to be better than both systems compared with DCAD and WPCA.

Hosseinpour et al. [60] presented a novel architecture for an intrusion detection system based on the artificial immune system, they proposed innate immunity using unsupervised machine learning methods, they have used DBSCAN clustering for its robustness and its great potential in classification. Then they evaluate the efficiency of both DBSCAN and K-means clustering algorithms. Results showed that DBSCAN detected correct traffic with the average false positive rate of 0.008 and true negative rate of 0.991 while K-mean detected same traffic with false positive rate of 0.156 and true negative rate of 0.843.

In [128] Singh and the team proposed a hybrid artificial immune system for IDS based on Support Vector Machine (SVM). The results of comparing traditional classification methods SVM and Dendritic Cell Algorithm (DCA) with the proposed hybrid model show increases in the accuracy rate by encapsulating SVM and DCA along with belief function method. SVM & DCA classification algorithm alone having accuracy rate for attack detection around 92.00% whereas hybrid model having accuracy rate up to 96.00%.

Shanmugam and Idris [209] provided a great survey on IDSs in literature and summarized most of the results achieved by researchers. Then writers provided results of the test for their proposed hybrid intelligent system

using fuzzy logic system, in these test the detection rate was 88.71% while false positive rate was 6.1%.

Shanmugavadivu and Nagarajan [148] developed an anomaly based intrusion detection system using fuzzy decision-making module for building attack detection capabilities. Analysing the result, the overall performance of the proposed system using KDD Cup 10% dataset was quite good since results show more than 90% accuracy for all types of attacks.

Obinna Igbe and Tarek Saadawi [137] present an anomaly detection system for detecting insider threat activities in an organization using an ensemble that consists of negative selection algorithms. Proposed system was able to classify the input data with a TPR of 83.45%, an FPR of 5.60%, an accuracy of 89.00%, and an area under the curve (AUC) value of 86.34%.

Saurabh and Verma [139] presents Immunity Inspired Cooperative Agent based Security System (IICASS) that uses Enhanced Negative Selection Algorithm (E-RNS) which incorporate fine tuning of detectors and detector power in negative selection algorithm. All the experiments use KDD Cup dataset for training and testing purposes. TS is composed of 972,781 normal records while TeS is composed of 5000 randomly selected unseen data, which includes both normal and attack data. The results illustrate effect of training samples in detection when it is varied from 25% to 100%.

Nguyen1 et al., [140] introduced a deep learning based bio-inspired algorithms that achieves an average detection rate of 98.8% over an experimental dataset of total around 9300 software binaries. In [138] Ortuño and a team proposed an intrusion detection systems framework using artificial immune system, the proposed system achieving an accuracy of 77%, with an execution time of 91.8 seconds per model.

Other promising efforts are done by Yan and Yu [210] in their work "AINIDS: an immune-based network intrusion detection system" which obtained 88% of accuracy. Xiaojie Jinquan Zeng et al. [211] in their anomaly detection framework using negative selection algorithm obtained 88% of correct classification, while Itzhak Levin [212] obtained around 92% of accuracy.

CHAPTER SIX

CONCLUSION AND FUTURE WORK

6. Conclusion and Future Work

6.1 Conclusion

Biological immune system is a very powerful intelligent system, with very complex interdisciplinary paradigm. The great interaction among different immune system cells, organs and molecules distributed all around the body without any central control lead up to a very strong detection system able to detect even unknown pathogens.

A relatively new computational intelligence system called artificial immune system created from the biological immune system and inspired by the great features of the immune system like anomaly detection, recognition of foreigners, adaptability, imperfect detection, memory, multi layered, diversity, dynamic learning, autonomy, optimization, parallel detection and others. Researchers heavily used AIS metaphor to model and design solutions to complex engineering problems especially in anomaly detection, optimization and classification. Since immune system itself is a very successful protection system, artificial immune system is used frequently in computer and network security applications especially IDS.

This thesis, presented a work in progress to model a network defence mechanism inspired by human immune system theory which known of its great protection capabilities. The proposed system is a multi-layer system composing of two main layers of defence working separately but still in a cooperative way, the system contains one more layer of defence called co-stimulation inspired by human immune system second signal and acting as a rechecking point. The first layer is the innate component, which is the first line of defence, fuzzy expert system used to imitate human innate main features, mechanisms and behaviour. The second layer of defence, the adaptive immune system component which is modelled and designed using well known basic theories like immune system network, negative

selection and clonal selection algorithms, is starting its mission to detect attacks and threats only after receiving a trigger from the innate component.

This work has been motivated by the challenges facing current intrusion detection systems in detecting and neutralizing new attacks and dealing with abnormal behaviours. Anomaly based IDSs research unlike the signature based IDSs have higher false positive detection rate and still needed more development to reach accepted level.

By building this framework, the intension was to develop one defence capability with multi-layered abilities of defence in which each layer is defending in a totally different way, the motivation here is to make one simple box for network protection instead of having firewall, antivirus and IDS/IPS (signature and anomaly based).

This research is motivated also by the desire and enthusiasm of the researcher to be part of the AIS development research. Although AIS is a very promising and growing research area inspired by a very powerful biological immune system characteristics, but still it needs more research efforts specially in developing new frameworks and algorithms.

The first hypothesis of this thesis was that by incorporating properties of both innate and adaptive immune systems into AIS this will enhance the performance of the system. The second hypothesis was that integrating different computational intelligent techniques is very useful for overcoming individual limitations and weaknesses, and this will lead to a powerful hybrid intelligent system. The evidences presented in details in this thesis supports both hypothesises.

In this thesis the AIS research was carefully reviewed. Although AIS was relatively new computational intelligent system but was clearly noticed a great achievements accomplished in solving complex engineering problems while still there is a big room of improvements. In this research, the important opinions of the AIS researchers on the progress of this rich

research field was reflected. Many researchers argue that the research of AIS has open issues still need to overcome in order to become a real world problem solving technique, those issues are described in details in chapter 2 of this thesis. This research is agreed generally with some aspects as a way forward for AIS as a promising intelligent system, such as:

- Working on new immune mechanisms and algorithms and develop general AIS frameworks, these cannot be achieved without a significant efforts to understanding the nature of AIS;
- Using cooperative frameworks incorporating innate immunity not only adaptive immune system;
- Using hybrid intelligent systems composing AIS and one of the soft computing techniques like fuzzy logic, genetic algorithm or neural network;
- Immunologists and computational scientists need to work together to improve the research of AIS.
- Building AISs based on biologically-realistic systemic models of the immune system, not only extracting and mimicking specific properties.

Four different experiments were conducted to test and validate the detection capabilities of the system; two for the innate component testing attacks from KDD'99 dataset and attacks generated in a lab, and the third test is for the adaptive component alone to have a bigger picture of the whole system. The last test conducted is simulating the adaptive layer after co-stimulation component. Innate component results show the ability of the system to deal with more than 79% of the traffic, and left less than 21% to the adaptive component with the false positive rate of 1.7% and false negative rate of only 0.73% and detection rate of about 97.79% and accuracy rate of 98.44%, and when passing the rest of the traffic to the adaptive component the system correctly recognizes 92.2% of the traffic

with false positive rate of 6.78% with detection rate of 96% and accuracy rate of 94%.

Once results obtained from adaptive layer, they have been rechecked using co-stimulation test, this test shows excellent results with false positive rate of only 0.78% and false negative rate of 0.89%.

Three extra tests were added to benchmark system detection accuracy with other dataset called NSL-KDD dataset, which considered as an updated and enhanced version of KDD'99 dataset. Results showed kind of similarity with the previous tests although the system was not trained with the NSL-KDD dataset, this is for sure very encouraging and proof the quality and validation of the framework.

Tests generally showed very encouraging results for both innate and adaptive components, and even better results are expected when adding more accurate rules to the innate knowledge base and allowing more training time to the adaptive layer.

Results clearly showed that incorporating properties of biological innate immune system into artificial immune system especially in computer security applications lead to a very effective systems and perform better than systems with only adaptive immunity. This thesis embraced a proved hypothesis that the innate immunity is largely responsible for triggering and directing adaptive response.

The proposed framework incorporated the features of innate system and adaptive systems together to represent real biological immune system powerful protection capabilities. Also fuzzy logic system together with AIS used since using hybrid intelligent systems help overcoming individual limitations and providing optional intelligent techniques to the designers. One more important feature of AIS is used to improve the quality of the output of the whole system by adding a co-stimulation layer as a verification second signal.

This research has also provided a general review of IDS, the research focused on the challenges and limitations of different types of IDSs as one of the important components of the modern information networks. The proposed multilayer framework has tried to overcome main IDS limitations like the difficulties it faces to detect unknown anomalies and the high false positive rate.

This thesis with other similar AIS based framework solutions, has provided a foundation on which AIS researchers can develop novel and useful solutions to real world challenged problems.

6.2 Contributions

Two major contributions can be noticed in this research:

a) A hybrid intelligent multilayer network defence framework inspired by artificial immune system algorithms incorporating both innate and adaptive immune systems. The developed system is providing intrusion detection and protection capabilities and can react to both known and unknown anomalies.
b) Modelling biological innate immune system response using fuzzy rule base system.

The following lists other contributions in this dissertation:

c) More than 3000 rule added to the knowledge base of the fuzzy logic system extracted from the behaviour of attacks and normal connections and by analysing daily network traffic.
d) This thesis provided a comprehensive literature review to the AIS theory with deep analysis of the evolution of the field including recent advances. Then the thesis suggested the way forward to better advancing the AIS applications, theories, algorithms and frameworks to the next level.
e) The proposed framework is a cooperative system since the knowledge base rules in the innate component and detectors in

adaptive component can be shared with other similar systems installed in different networks.

f) The system suggested some solutions to the inherited drawbacks of the KDD'99 dataset used in the training and tests instances.

g) In the adaptive layer, costimulation signal used to both innate and adaptive components, this will enhance the detection rates for normal and abnormal traffic.

6.3 Future Work

All the experiments in this thesis were conducted offline, no experiments on a real network infrastructure were performed, and this for sure limited the analysis to be only performed on the simulations results. The plan is to prepare the system in the future to be working online in a local network environment then later test it in a real information network. Running the proposed network defence system in a real network needed a lot of work starting by preparing the Input Unit to receive huge number of connections and extract features from them, it is important then to minimize the size and number of detectors to reduce time for comparing bit strings in the adaptive immune system then other steps will follow.

This research was intended basically to contribute on the innate immune layer whereas basic and typical adaptive layer has been applied as a second layer of defence. The research was also intended to incorporate innate and adaptive responses as a two layers of defence. In the future more focus on the adaptive layer mechanisms and algorithms needed, this may enhance the overall performance of the framework.

One of the main areas needed more investigations is the length of the binary strings that represent the detectors and self and non-self-sets for the IDS in a network environment as well as a number and distribution of the detectors. A large number of detectors or/and big representation size could be needed to guarantee a good level of detection but for sure it will

consume huge resources, so more works need to be added on finding a better set of compromising parameters.

In the experiments performed six performance evaluation metrics were adopted, including confusion metrics, detection rate and accuracy rate. The evaluation tests been analyzed was only concentrated on the correctness of the system so several metrics have to be considered in the future to better measure the effectiveness as well. The proposed metrics may include: recall (R), precision (P), F-measure (FM), cost per example (CPE), intrusion detection capability (CID) and area under curve (AUC). It is vital also to evaluate the network performance after installing the proposed system, network performance measurement parameters to be evaluated could include but not limited to: latency, packet loss, throughput, bandwidth and jitter.

REFERENCES

Published Papers

[1] Elhaj, M.M., Hamrawi, H. and Suliman, M.M., 2013, August. A multi-layer network defense system using artificial immune system. In 2013 International Conference on Computing, Electrical and Electronic Engineering (ICCEEE) (pp. 232-236). IEEE.

[2] Elhaj, M.M, Hamrawi, H. and Abdalla, Y., 2016. A Novel Multilayer Artificial Immune System for Network Defense. International Journal of Scientific & Engineering Research, Volume 7, Issue 2, ISSN 2229-5518.

[3] Elhaj, M.M, Hamrawi, H. and Abdalla, Y., 2020. Review of Artificial Immune System Research. International Journal of Scientific & Engineering Research, Volume 11, Issue 1, ISSN 2229-5518.

References

[1] Twycross, J. and Aickelin, U., 2005, August. Towards a conceptual framework for innate immunity. In International Conference on Artificial Immune Systems (pp. 112-125). Springer, Berlin, Heidelberg.

[2] Engelbrecht, A.P., 2007. Computational intelligence: an introduction. John Wiley & Sons.

[3] Siddique, N. and Adeli, H., 2013. Computational intelligence: synergies of fuzzy logic, neural networks and evolutionary computing. John Wiley & Sons.

[4] Revathi, M. and Arthi, K., 2014. Application of Artificial Immune System Algorithms in Dataset Classification. International Journal of Innovative Research in Advanced Engineering (IJIRAE), 1(6), pp.291-293.

[5] De Castro, L.N. and Von Zuben, F.J., 1999. Artificial immune systems: Part I–basic theory and applications. Universidade Estadual de Campinas, Dezembro de, Tech. Rep, 210(1).

[6] Zhang, C., Zhang, J., Liu, S. and Liu, Y., 2008, October. Network intrusion active defense model based on artificial immune system. In 2008 Fourth International Conference on Natural Computation (Vol. 1, pp. 97-100). IEEE.

[7] Zhang, Q.H., Zhang, Y.S., Shao, L.Q., Fu, Y.Z., Li, H.F. and Liang, B.L., 2008, December. An immunity-based technical research into network intrusion detection. In 2008 International Conference on Computer Science and Software Engineering (Vol. 3, pp. 955-958). IEEE.

[8] Daudi J. An., 2015. An Overview of Application of Artificial Immune System in Swarm Robotic Systems. Advances in Robotics & Automation.

[9] Read M., Andrews P.S., Timmis J., 2012. An Introduction to Artificial Immune Systems. In: Rozenberg G., Bäck T., Kok J.N. (eds) Handbook of Natural Computing. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-92910-9_47.

[10] Al-Enezi, J., 2012. Artificial immune systems based committee machine for classification application (Doctoral dissertation, Brunel University School of Engineering and Design PhD Theses).

[11] Su, M.C., Wang, P.C. and Yang, Y.S., 2008. A new approach to artificial immune systems and its application in constructing on-line learning neuro-fuzzy systems. The Open Artificial Intelligence Journal, 2(1).

[12] Greensmith, J., Whitbrook, A. and Aickelin, U., 2010. Artificial immune systems. In Handbook of Metaheuristics (pp. 421-448). Springer, Boston, MA.

[13] Harmer, P.K., Williams, P.D., Gunsch, G.H. and Lamont, G.B., 2002. An artificial immune system architecture for computer security

applications. IEEE transactions on evolutionary computation, 6(3), pp.252-280.

[14] González, F. and Dasgupta, D., 2003. A study of artificial immune systems applied to anomaly detection (Doctoral dissertation, University of Memphis).

[15] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G. and Vázquez, E., 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, 28(1-2), pp.18-28.

[16] Kayacik, H.G. and Zincir-Heywood, A.N., 2006, October. Using self-organizing maps to build an attack map for forensic analysis. In Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services (pp. 1-8).

[17] Hart, E. and Timmis, J., 2008. Application areas of AIS: The past, the present and the future. Applied soft computing, 8(1), pp.191-201.

[18] Bezdek, J.C., 1994. What is computational intelligence? (No. CONF-9410335). USDOE Pittsburgh Energy Technology Center, PA (United States); Oregon State Univ., Corvallis, OR (United States). Dept. of Computer Science; Naval Research Lab., Washington, DC (United States); Electric Power Research Inst., Palo Alto, CA (United States); Bureau of Mines, Washington, DC (United States).

[19] Elhaj, M.M, Hamrawi, H. and Abdalla, Y., 2016. A Novel Multilayer Artificial Immune System for Network Defense. International Journal of Scientific & Engineering Research, Volume 7, Issue 2, ISSN 2229-5518.

[20] Wang, W., Gao, S., Li, F. and Tang, Z., 2008. A complex artificial immune system and its immunity. International Journal of Computer Science and Network Security, 8, pp.287-295.

[21] Igbe, O., 2019. Artificial immune system based approach to cyber attack detection (Doctoral dissertation, The City College of New York).

[22] Al-Enezi, J.R., Abbod, M.F. and Alsharhan, S., 2010. Artificial immune systems-models, algorithms and applications.

[23] Mishra, P.K. and Bhusry, M., 2015. Artificial immune system: State of the art approach. International Journal of Computer Applications, 120(20).

[24] Hajela, P., Yoo, J. and Lee, J., 1997. GA based simulation of immune networks applications in structural optimization. Engineering Optimization, 29(1-4), pp.131-149.

[25] Nasaroui, O., Gonzalez, F. and Dasgupta, D., 2002, May. The fuzzy artificial immune system: Motivations, basic concepts, and application to clustering and web profiling. In 2002 IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems. FUZZ-IEEE'02. Proceedings (Cat. No. 02CH37291) (Vol. 1, pp. 711-716). IEEE.

[26] Vargas, P.A., de Castro, L.N., Michelan, R. and Von Zuben, F.J., 2003, September. An immune learning classifier network for autonomous navigation. In International Conference on Artificial Immune Systems (pp. 69-80). Springer, Berlin, Heidelberg.

[27] Xian, J.Q., Lang, F.H. and Tang, X.L., 2005, August. A novel intrusion detection method based on clonal selection clustering algorithm. In 2005 International conference on machine learning and cybernetics (Vol. 6, pp. 3905-3910). IEEE.

[28] Karakasis, V.K. and Stafylopatis, A., 2006, July. Data mining based on gene expression programming and clonal selection. In 2006 IEEE International Conference on Evolutionary Computation (pp. 514-521). IEEE.

[29] Fu, J., Li, Z. and Tan, H.Z., 2007, July. A hybrid artificial immune network with swarm learning. In 2007 International Conference on Communications, Circuits and Systems (pp. 910-914). IEEE.

[30] Gan, Z., Yang, Z., Li, G. and Jiang, M., 2007, August. Automatic modeling of complex functions with clonal selection-based gene expression programming. In Third International Conference on Natural Computation (ICNC 2007) (Vol. 4, pp. 228-232). IEEE.

[31] Gu, D., Ai, Q. and Chen, C., 2008, April. The application of artificial immune network in load classification. In 2008 Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (pp. 1394-1398). IEEE.

[32] Smith, R.E., Timmis, J., Stepney, S. and Neal, M., 2005. Conceptual frameworks for artificial immune systems. International Journal of Unconventional Computing, 1(3), pp.315-338.

[33] Bateni, M., Baraani, A. and Ghorbani, A., 2013. Using Artificial Immune System and Fuzzy Logic for Alert Correlation. IJ Network Security, 15(3), pp.190-204.

[34] Sanyal, S. and Thakur, M.R., 2012. A Hybrid Approach towards Intrusion Detection Based on Artificial Immune System and Soft Computing, pp.1205.4457.

[35] Shamshirband, S., Anuar, N.B., Kiah, M.L.M., Rohani, V.A., Petković, D., Misra, S. and Khan, A.N., 2014. Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. Journal of Network and Computer Applications, 42, pp.102-117.

[36] Shih, C.J. and Kuan, T.L., 2008. Immune based hybrid evolutionary algorithm for Pareto engineering optimization. Journal of Applied Science and Engineering, 11(4), pp.395-402.

[37] Liu, Y., 2009. A neuro-immune inspired computational framework and its applications to a machine visual tracking system (Doctoral dissertation, University of York).

[38] Tarakanov, A. and Dasgupta, D., 2000. A formal model of an artificial immune system. BioSystems, 55(1-3), pp.151-158.

[39] Dasgupta, D., 2006. Advances in artificial immune systems. IEEE computational intelligence magazine, 1(4), pp.40-49.

[40] Mihaljevic, B., Cvitas, A. and Zagar, M., 2006, June. Recommender system model based on artificial immune system. In 28th International Conference on Information Technology Interfaces, 2006. (pp. 367-372). IEEE.

[41] Hosseinpour, F., Bakar, K.A., Hardoroudi, A.H. and Kazazi, N., 2010, November. Survey on artificial immune system as a bio-inspired technique for anomaly based intrusion detection systems. In 2010 International Conference on Intelligent Networking and Collaborative Systems (pp. 323-324). IEEE.

[42] Axelsson, S., 2000. Intrusion detection systems: A survey and taxonomy (Vol. 99). Technical report.

[43] Timmis, J., Andrews, P., Owens, N. and Clark, E., 2008, August. Immune systems and computation: An interdisciplinary adventure. In International Conference on Unconventional Computation (pp. 8-18). Springer, Berlin, Heidelberg.

[44] Dasgupta, D., Yu, S. and Nino, F., 2011. Recent advances in artificial immune systems: models and applications. Applied Soft Computing, 11(2), pp.1574-1587.

[45] Timmis, J., 2000. Artificial immune systems: A novel data analysis technique inspired by the immune network theory (Doctoral dissertation, Department of Computer Science).

[46] Dasgupta, D., 1993. An overview of artificial immune systems and their applications. In Artificial immune systems and their applications (pp. 3-21). Springer, Berlin, Heidelberg.

[47] Castro, L.N., De Castro, L.N. and Timmis, J., 2002. Artificial immune systems: a new computational intelligence approach. Springer Science & Business Media.

[48] Timmis, J., Knight, T., de Castro, L.N. and Hart, E., 2004. An overview of artificial immune systems. In Computation in Cells and Tissues (pp. 51-91). Springer, Berlin, Heidelberg.

[49] Goodman, D.E., Boggess, L. and Watkins, A., 2002. Artificial immune system classification of multiple-class problems. Proceedings of the artificial neural networks in engineering ANNIE, 2(2002), pp.179-183.

[50] Wang, L., Ma, S. and Hei, X.H., 2008, December. Research on an immune mechanism based intelligent spam filter. In 2008 International Conference on Computer Science and Software Engineering (Vol. 3, pp. 673-676). IEEE.

[51] Beri, S.A.A., 2014. An Artificial Immune Classification and Clustering Systems: A Survey.

[52] ME, S.C. and Rajaram, M., 2008. A Software Reliability Estimation Tool Using Artificial Immune Recognition System. In Proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1).

[53] Rana, Ritesh & Meelu, Punita., 2013. A review of Artificial Immune System for Network IDS. www.ijcst.com. 4.

[54] Somayaji, A., Hofmeyr, S. and Forrest, S., 1998, January. Principles of a computer immune system. In Proceedings of the 1997 workshop on New security paradigms (pp. 75-82).

[55] Hamza, A. and Hussain, D.J., 2014. Computer virus detection based on artificial immunity concept. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(2), pp.68-74

[56] Hofmeyr, S.A. and Forrest, S., 1999, July. Immunity by design: An artificial immune system. In Proceedings of the 1st Annual Conference on Genetic and Evolutionary Computation-Volume 2 (pp. 1289-1296).

[57] Yeom, K.W. and Park, J.H., 2006, August. An artificial immune system model for multi agents based resource discovery in distributed environments. In First International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06) (Vol. 1, pp. 234-239). IEEE.

[58] Kim, J. and Bentley, P., 1999, September. The human immune system and network intrusion detection. In 7th European Conference on Intelligent Techniques and Soft Computing (EUFIT'99), Aachen, Germany (pp. 1244-1252).

[59] King, R.L., Russ, S.H., Lambert, A.B. and Reese, D.S., 2001. An artificial immune system model for intelligent agents. Future Generation Computer Systems, 17(4), pp.335-343.

[60] Hosseinpour, F., Amoli, P.V., Farahnakian, F., Plosila, J. and Hämäläinen, T., 2014. Artificial immune system based intrusion detection: Innate immunity using an unsupervised learning approach. International Journal of Digital Content Technology and its Applications, 8(5), p.1.

[61] Muda, A.K. and Shamsuddin, S.M., 2005. An overview of artificial immune system in pattern recognition. In Proceedings of the Postgraduate Annual Research Seminar, In (pp. 119-126).

[62] Khairi, R.S., 2015. Artificial immune system based on real valued negative selection algorithms for anomaly detection (Doctoral dissertation, Universiti Tun Hussein Onn Malaysia).

[63] Guillen, E. and Paez, R., 2010, December. Artificial Immune Systems–AIS as Security Network Solution. In International Conference on Bio-Inspired Models of Network, Information, and Computing Systems (pp. 680-681). Springer, Berlin, Heidelberg.

[64] Twycross, J. and Aickelin, U., 2007, August. Biological inspiration for artificial immune systems. In International Conference on Artificial Immune Systems (pp. 300-311). Springer, Berlin, Heidelberg.

[65] Forrest, S. and Beauchemin, C., 2007. Computer immunology. Immunological reviews, 216(1), pp.176-197.

[66] Andrews, P.S. and Timmis, J., 2005, August. Inspiration for the next generation of artificial immune systems. In International Conference on

Artificial Immune Systems (pp. 126-138). Springer, Berlin, Heidelberg.

[67] Bersini, H., 2006, September. Immune system modeling: The OO way. In International Conference on Artificial Immune Systems (pp. 150-163). Springer, Berlin, Heidelberg.

[68] Timmis, J., 2007. Artificial immune systems—today and tomorrow. Natural computing, 6(1), pp.1-18.

[69] Cohen, I.R., 2007. Real and artificial immune systems: computing the state of the body. Nature Reviews Immunology, 7(7), pp.569-574.

[70] Burnet, S.F.M., 1959. The clonal selection theory of acquired immunity (Vol. 3). Nashville: Vanderbilt University Press.

[71] Jerne, N.K., 1974. Towards a network theory of the immune system. Ann. Immunol., 125, pp.373-389.

[72] Zheng, J., Chen, Y. and Zhang, W., 2010. A survey of artificial immune applications. Artificial Intelligence Review, 34(1), pp.19-34.

[73] Radosavac, S., 2002. Detection and classification of network intrusions using hidden markov models (No. ISR-MS-2003-1). Maryland Univ. College Park Inst. for Systems Research.

[74] Cohen, I.R., 2000. Tending Adam's Garden: evolving the cognitive immune self. Elsevier.

[75] Timmis, J., Andrews, P., Owens, N. and Clark, E., 2008. An interdisciplinary perspective on artificial immune systems. Evolutionary Intelligence, 1(1), pp.5-26.

[76] Freitas, Alex & Timmis, Jon., 2003. Revisiting the Foundations of Artificial Immune Systems: A Problem-Oriented Perspective. 229-241. 10.1007/978-3-540-45192-1_22.

[77] Abi Haidar, A., Six, A., Ganascia, J.G. and Thomas-Vaslin, V., 2013, September. The artificial immune systems domain: identifying progress and main contributors using publication and co-authorship analyses. In Artificial Life Conference Proceedings 13 (pp. 1206-1217). One Rogers Street, Cambridge, MA 02142-1209 USA journals-info@ mit. edu: MIT Press.

[78] Alaparthy, V.T., Amouri, A. and Morgera, S.D., 2018. A study on the adaptability of immune models for wireless sensor network security. Procedia computer science, 145, pp.13-19.

[79] Fister, Karin & Fister jr, Iztok & Fister, Iztok., 2013. Immune systems in computer science. Anali PAZU. 3.

[80] Yang, H., Li, T., Hu, X., Wang, F. and Zou, Y., 2014. A survey of artificial immune system based intrusion detection. The Scientific World Journal, 2014.

[81] Ishida, Y., 1990, June. Fully distributed diagnosis by PDP learning algorithm: towards immune network PDP model. In 1990 IJCNN International Joint Conference on Neural Networks (pp. 777-782). IEEE.

[82] Forrest, S., Perelson, A.S., Allen, L. and Cherukuri, R., 1994, May. Self-nonself discrimination in a computer. In Proceedings of 1994 IEEE computer society symposium on research in security and privacy (pp. 202-212). Ieee.

[83] Yang, J., Wang, T., MingLiu, C. and Li, B., 2011, March. Improved Agent Model for Network Security Evaluation Based on AIS. In 2011 Fourth International Conference on Intelligent Computation Technology and Automation (Vol. 1, pp. 151-154). IEEE.

[84] Zheng, X., Fang, Y., Zhou, Y. and Zhang, J., 2013. A novel multi-layered immune network intrusion detection defense model: MINID. Journal of Networks, 8(3), p.636.

[85] Chao, R. and Tan, Y., 2009, December. A virus detection system based on artificial immune system. In 2009 international conference on computational intelligence and security (Vol. 1, pp. 6-10). IEEE.

[86] De Castro, L.N. and Von Zuben, F.J., 2000. Artificial immune systems: Part II–A survey of applications. FEEC/Univ. Campinas, Campinas, Brazil.

[87] Dasgupta, D., 1996. Using immunological principles in anomaly detection. Proceedings of the Artificial Neural Networks in Engineering (ANNIE'96), St. Louis, USA.

[88] Seredynski, F. and Bouvry, P., 2007. Anomaly detection in TCP/IP networks using immune systems paradigm. Computer communications, 30(4), pp.740-749.

[89] Twycross, J.P., 2007. Integrated innate and adaptive artificial immune systems applied to process anomaly detection (Doctoral dissertation, University of Nottingham).

[90] Hang, X. and Dai, H., 2005, June. Applying both positive and negative selection to supervised learning for anomaly detection. In Proceedings of the 7th annual conference on Genetic and evolutionary computation (pp. 345-352).

[91] de Castro, L.N. and Von Zuben, F.J., 2002. aiNet: an artificial immune network for data analysis. In Data mining: a heuristic approach (pp. 231-260). IGI Global.

[92] Cao, Y. and Dasgupta, D., 2003. An immunogenetic approach in chemical spectrum recognition. In Advances in evolutionary computing (pp. 897-914). Springer, Berlin, Heidelberg.

[93] Kalmanje, K.K. and Neidhoefer, J., 1999. Immunized adaptive critic for an autonomous aircraft control application. In Artificial immune systems and their applications (pp. 221-241). Springer, Berlin, Heidelberg.

[94] Kelsey, J. and Timmis, J., 2003, July. Immune inspired somatic contiguous hypermutation for function optimisation. In Genetic and Evolutionary Computation Conference (pp. 207-218). Springer, Berlin, Heidelberg.

[95] Mori, K., Tsukiyama, M. and Fukuda, T., 1996. Multi-Optimization by Immune Algorithm with Diversity and Learning. 2nd Int. Conf. on

Multi-Agent Systems. In Workshop Notes on Immunity-Based Systems (pp. 118-123).

[96] De Castro, L.N. and Timmis, J., 2002, May. An artificial immune network for multimodal function optimization. In Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No. 02TH8600) (Vol. 1, pp. 699-704). IEEE.

[97] Bradley, D.W. and Tyrrell, A.M., 2000, April. Immunotronics: Hardware fault tolerance inspired by the immune system. In International Conference on Evolvable Systems (pp. 11-20). Springer, Berlin, Heidelberg.

[98] Dasgupta, D., Krishna Kumar, K., Wong, D. and Berry, M., 2004, September. Negative selection algorithm for aircraft fault detection. In International Conference on Artificial Immune Systems (pp. 1-13). Springer, Berlin, Heidelberg.

[99] Zhang, C. and Yi, Z., 2007, June. An artificial immune network model applied to data clustering and classification. In International Symposium on Neural Networks (pp. 526-533). Springer, Berlin, Heidelberg.

[100] De Casto, L.N. and Von Zuben, F.J., 2000, November. An evolutionary immune network for data clustering. In Proceedings. Vol. 1. Sixth Brazilian Symposium on Neural Networks (pp. 84-89). IEEE.

[101] Wierzchoń, S.T. and Kużelewska, U., 2002. Stable clusters formation in an artificial immune system. In Conference on AIS, University of Kent at Canterbury, UK (pp. 9-11).

[102] Viswalingam, Dr. Kathir & appan, G.Ayy., 2015. A Study and Survey of Artificial Immune Systems. International Journal of Innovative Research in Computer and Communication Engineering. 02. 7197-7201. 10.15680/IJIRCCE.2014.0212010.

[103] Song, Y., Kołcz, A. and Giles, C.L., 2009. Better Naive Bayes classification for high-precision spam detection. Software: Practice and Experience, 39(11), pp.1003-1024.

[104] Dudek, G., 2012. An artificial immune system for classification with local feature selection. IEEE Transactions on Evolutionary Computation, 16(6), pp.847-860.

[105] Watkins, A., Timmis, J. and Boggess, L., 2004. Artificial immune recognition system (AIRS): An immune-inspired supervised learning algorithm. Genetic Programming and Evolvable Machines, 5(3), pp.291-317.

[106] Hart, E., Ross, P. and Nelson, J., 1998, May. Producing robust schedules via an artificial immune system. In 1998 IEEE International Conference on Evolutionary Computation Proceedings. IEEE World Congress on Computational Intelligence (Cat. No. 98TH8360) (pp. 464-469). IEEE.

[107] Vijeta, Vivek Sharma, 2014, A Review on Network Intrusion Detection using Artificial Immune System (AIS), International Journal of Engineering Research & Technology (IJERT) Volume 03, Issue 04.

[108] Chauhan, P., Singh, N. and Chandra, N., 2013. A Review on Intrusion Detection System based on Artificial Immune System. International Journal of Computer Applications, 63(20).

[109] Rui, L. and Wanbo, L., 2010, July. Intrusion response model based on AIS. In 2010 International forum on information technology and applications (Vol. 1, pp. 86-90). IEEE.

[110] Ehret, C. and Ultes-Nitsche, U., 2008. Immune system based intrusion detection system. In Innovative Minds (Information Systems Security Association-ISSA 2008), Johannesburg, South Africa, July 2008.

[111] Luther, K., Bye, R., Alpcan, T., Muller, A. and Albayrak, S., 2007, June. A cooperative AIS framework for intrusion detection. In 2007 IEEE International Conference on Communications (pp. 1409-1416). IEEE.

[112] Farhaoui, Y., 2017. Design and implementation of an intrusion prevention system. International Journal of Network Security, 19(5), pp.675-683.

[113] Song, K., Kim, P., Tyagi, V. and Rajasekaran, S., 2018. Artificial Immune System (AIS) Based Intrusion Detection System (IDS) for Smart Grid Advanced Metering Infrastructure (AMI) Networks.

[114] Aydın, M.A., Zaim, A.H. and Ceylan, K.G., 2009. A hybrid intrusion detection system design for computer network security. Computers & Electrical Engineering, 35(3), pp.517-526.

[115] Bashah, N., Shanmugam, I.B. and Ahmed, A.M., 2005. Hybrid intelligent intrusion detection system. World Academy of Science, Engineering and Technology, 11, pp.23-26.

[116] Benyettou, N., Benyettou, A., ROdIN, V.I.N.C.E.N.T. and Berrouiguet, S.Y., 2013. The multi-agents immune system for network intrusions detection (MAISID). Oriental Journal of Computer Science & Technology, 6(4), pp.383-390.

[117] Shen, J. and Wang, J., 2011, November. Network intrusion detection by artificial immune system. In IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society (pp. 4716-4720). IEEE.

[118] Bebo, J.L., 2002. Using Relational Schemata in a Computer Immune System to Detect Multiple-Packet Network Intrusions (No. AFIT/GCS/ENG/02M-02). Air Force Inst. of Tech Wright-Patterson AFB OH School of Engineering and Management.

[119] Powers, S.T. and He, J., 2008. A hybrid artificial immune system and Self Organising Map for network intrusion detection. Information Sciences, 178(15), pp.3024-3042.

[120] Kim, J., Bentley, P.J., Aickelin, U., Greensmith, J., Tedesco, G. and Twycross, J., 2007. Immune system approaches to intrusion detection–a review. Natural computing, 6(4), pp.413-466.

[121] Jiandong, G., Zhiguang, Q. and Lin, Z., 2005, December. An approach of AIS LAN based on Intel IXP2800. In Second International Conference on Embedded Software and Systems (ICESS'05) (pp. 6-pp). IEEE.

[122] Dasgupta, D., 1999, October. Immunity-based intrusion detection system: A general framework. In Proc. of the 22nd NISSC (Vol. 1, pp. 147-160).

[123] Middlemiss, M. and Whigham, P.A., 2006, October. Innate and adaptive principles for an artificial immune system. In Asia-Pacific Conference on Simulated Evolution and Learning (pp. 88-95). Springer, Berlin, Heidelberg.

[124] Twycross, J., Aickelin, U. and Whitbrook, A., 2010. Detecting anomalous process behaviour using second generation artificial immune systems. International Journal of Unconventional Computing, pp. 301.326.

[125] Qiang, H. and Yiqian, T., 2010, July. A Network Security Evaluate Method Base on AIS. In 2010 International Forum on Information Technology and Applications (Vol. 2, pp. 42-45). IEEE.

[126] Kim, J. and Bentley, P., 1999, September. The artificial immune model for network intrusion detection. In 7th European congress on intelligent techniques and soft computing (EUFIT'99) (Vol. 158).

[127] Sadeghi, Z. and Bahrami, A.S., 2013, May. Improving the speed of the network intrusion detection. In The 5th conference on information and knowledge technology (pp. 88-91). IEEE.

[128] Singh, S., Singh, J.P. and Shrivastva, G., 2013, July. A hybrid artificial immune system for IDS based on SVM and belief function. In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[129] Shen, J., Wang, J. and Ai, H., 2012. An improved artificial immune system-based network intrusion detection by using rough set.

[130] Zhang, Y., Wang, L., Sun, W., Green, R.C. and Alam, M., 2011, July. Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid. In 2011 IEEE Power and Energy Society General Meeting (pp. 1-8). IEEE.

[131] Tedesco, G., Twycross, J. and Aickelin, U., 2006, September. Integrating innate and adaptive immunity for intrusion detection. In International Conference on Artificial Immune Systems (pp. 193-202). Springer, Berlin, Heidelberg.

[132] Hofmeyr, S.A. and Forrest, S., 2000. Architecture for an artificial immune system. Evolutionary computation, 8(4), pp.443-473.

[133] Abas, E.A.E.R., Abdelkader, H. and Keshk, A., 2015, December. Artificial immune system based intrusion detection. In 2015 IEEE seventh international conference on intelligent computing and information systems (ICICIS) (pp. 542-546). IEEE.

[134] Aickelin, U., Bentley, P., Cayzer, S., Kim, J. and McLeod, J., 2003, September. Danger theory: The link between AIS and IDS?. In International Conference on Artificial Immune Systems (pp. 147-155). Springer, Berlin, Heidelberg.

[135] Chan, F.T., Prakash, A., Tibrewal, R.K. and Tiwari, M.K., 2013. Clonal selection approach for network intrusion detection. Singapore, April, pp.29-30.

[136] Igbe, O., Darwish, I. and Saadawi, T., 2016, June. Distributed network intrusion detection systems: An artificial immune system approach. In 2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE) (pp. 101-106). IEEE.

[137] Igbe, O. and Saadawi, T., 2018, November. Insider Threat Detection using an Artificial Immune system Algorithm. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 297-302). IEEE.

[138] Ortuño, S.Y., Hernández-Aguilar, J.A. and Zezzatti, C.A.O.O., 2016. Implementation of a Security Model for Malware Based on Artificial Immune System. Res. Comput. Sci., 122, pp.103-112.

[139] Saurabh, P. and Verma, B., 2018. Immunity inspired cooperative agent based security system. Int. Arab J. Inf. Technol., 15(2), pp.289-295.

[140] Nguyen, V.T. and Le Hoang Dung, T.D.L., 2018. A Combination of Artificial Immune System and Deep Learning for Virus Detection. International Journal of Applied Engineering Research, 13(22), pp.15622-15628.

[141] Akshay U. Mahajan and Nitin Y. Suryawanshi., 2017. Two Layer Artificial Immune System for Intrusion Detection System. International Conference Proceeding ICGTETM Dec 2017 | ISSN: 2320-2882.

[142] Dutt, I., Borah, S. and Maitra, I., 2016. Intrusion detection system using artificial immune system. International Journal of Computer Applications, 144(12).

[143] Behzad, S., Fotohi, R., Balov, J.H. and Rabipour, M.J., 2020. An artificial immune based approach for detection and isolation misbehavior attacks in wireless networks. arXiv preprint arXiv:2003.00870.

[144] Hellmann, M., 2001. Fuzzy logic introduction. Université de Rennes, 1.

[145] Elhaj, M.M., Hamrawi, H. and Suliman, M.M., 2013, August. A multi-layer network defense system using artificial immune system. In 2013 International Conference on Computing, Electrical and Electronic Engineering (ICCEEE) (pp. 232-236). IEEE.

[146] Tillapart, P., Thumthawatworn, T. and Santiprabhob, P., 2002. Fuzzy intrusion detection system. AU JT, 6(2), pp.109-114.

[147] Bridges, S.M., Vaughn, R.B. and Siraj, A., 2002. AI techniques applied to high performance computing intrusion detection. In Proceeding of the Tenth International Conference on Telecommunication Systems, Modeling and Analysis, Monterey CA (Vol. 2, pp. 100-114).

[148] Shanmugavadivu, R. and Nagarajan, N., 2011. Network intrusion detection system using fuzzy logic. Indian Journal of Computer Science and Engineering (IJCSE), 2(1), pp.101-111

[149] Dhanalakshmi, Y. and Babu, I.R., 2008. Intrusion detection using data mining along fuzzy logic and genetic algorithms. International Journal of Computer Science and Network Security, 8(2), pp.27-32.

[150] Lin, J., Huang, T. and Bingjie, Z., 2008, December. A fast fuzzy set intrusion detection model. In 2008 International Symposium on Knowledge Acquisition and Modeling (pp. 601-605). IEEE.

[151] Fachada, N., Lopes, V. and Rosa, A., 2007. Agent-based modelling and simulation of the immune system: a review. In EPIA 2007-13th Portuguese Conference on Artificial Intelligence.

[152] Rashid, N., Iqbal, J., Mahmood, F., Abid, A., Khan, U.S. and Tiwana, M.I., 2018. Artificial immune system–Negative selection classification algorithm (NSCA) for four class electroencephalogram (EEG) Signals. Frontiers in human neuroscience, 12, p.439.

[153] Mayer, G., 2009. Innate (non-specific) immunity. Immunology–chapter one. Microbiology and immunology textbook, pp.1-10.

[154] Krishnan, A., 2004. Modeling and Simulation of the Innate Immune System. Master Project Department of Computer Science University of Colorado at Colorado Springs Colorado, USA.

[155] EshghiShargh, A., 2009, November. Using artificial immune system on implementation of Intrusion detection systems. In 2009 Third UKSim European Symposium on Computer Modeling and Simulation (pp. 164-168). IEEE.

[156] Knight, T. and Timmis, J., 2003, November. A multi-layered immune inspired approach to data mining. In Proceedings of the 4th International Conference on Recent Advances in Soft Computing (Vol. 1, pp. 195-201).

[157] Germain, R.N., 2004. An innately interesting decade of research in immunology. Nature medicine, 10(12), pp.1307-1320.

[158] Chaudhary, P. and Kumar, K., 2018. Artificial Immune System: Algorithms and Applications Review. International Journal of Information and Communication Technology, 1(1).

[159] Dasgupta, D., Ji, Z. and Gonzalez, F., 2003, December. Artificial immune system (AIS) research in the last five years. In The 2003 Congress on Evolutionary Computation, 2003. CEC'03. (Vol. 1, pp. 123-130). IEEE.

[160] Ayara, M., Timmis, J., de Lemos, R., de Castro, L.N. and Duncan, R., 2002, September. Negative selection: How to generate detectors. In Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS) (Vol. 1, pp. 89-98). University of Kent at Canterbury Printing Unit University of Kent at Canterbury.

[161] Idris, I., 2012. Model and algorithm in artificial immune system for spam detection. International Journal of Artificial Intelligence & Applications, 3(1), p.83.

[162] Timmis, J., Neal, M. and Hunt, J., 2000. An artificial immune system for data analysis. Biosystems, 55(1-3), pp.143-150.

[163] Timmis, J. and Neal, M., 2001. A resource limited artificial immune system for data analysis. In Research and Development in Intelligent Systems XVII (pp. 19-32). Springer, London.

[164] Luh, G.C. and Liu, W.W., 2004, September. Reactive immune network based mobile robot navigation. In International Conference on Artificial Immune Systems (pp. 119-132). Springer, Berlin, Heidelberg.

[165] Neal, M., 2003, September. Meta-stable memory in an artificial immune network. In International Conference on Artificial Immune Systems (pp. 168-180). Springer, Berlin, Heidelberg.

[166] Secker, A., Freitas, A.A. and Timmis, J., 2003, December. AISEC: an artificial immune system for e-mail classification. In The 2003 Congress on Evolutionary Computation, 2003. CEC'03. (Vol. 1, pp. 131-138). IEEE.

[167] Alonso, O.M., Nino, F. and Velez, M., 2004, September. A robust immune based approach to the iterated prisoner's dilemma. In International Conference on Artificial Immune Systems (pp. 290-301). Springer, Berlin, Heidelberg.

[168] Tian, X., Yang, H.D. and Deng, F.Q., 2006, August. A novel artificial immune network algorithm. In 2006 international conference on machine learning and cybernetics (pp. 2159-2165). IEEE.

[169] Lv, J., 2007, August. Study on chaos immune network algorithm for multimodal function optimization. In Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007) (Vol. 3, pp. 684-689). IEEE.

[170] Huang, W. and Jiao, L., 2008. Artificial immune kernel clustering network for unsupervised image segmentation. Progress in Natural Science, 18(4), pp.455-461.

[171] D'haeseleer, P., Forrest, S. and Helman, P., 1996, May. An immunological approach to change detection: algorithms, analysis and implications. In Proceedings 1996 IEEE Symposium on Security and Privacy (pp. 110-119). IEEE.

[172] Mahboubian, M., Udzir, N.I., Subramaniam, S. and Hamid, N.A.W.A., 2012, June. An alert fusion model inspired by artificial immune system. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 317-322). IEEE.

[173] Aydin, I., Karakose, M. and Akin, E., 2010. Chaotic-based hybrid negative selection algorithm and its applications in fault and anomaly detection. Expert Systems with Applications, 37(7), pp.5285-5294.

[174] Gong, M., Zhang, J., Ma, J. and Jiao, L., 2012. An efficient negative selection algorithm with further training for anomaly detection. Knowledge-Based Systems, 30, pp.185-191.

[175] Igawa, K. and Ohashi, H., 2009. A negative selection algorithm for classification and reduction of the noise effect. Applied Soft Computing, 9(1), pp.431-438.

[176] Gonzales, L.J. and Cannady, J., 2004, June. A self-adaptive negative selection approach for anomaly detection. In Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No. 04TH8753) (Vol. 2, pp. 1561-1568). IEEE.

[177] Esponda, F., Forrest, S. and Helman, P., 2004. A formal framework for positive and negative detection schemes. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 34(1), pp.357-373.

[178] Gong, M., Jiao, L., Zhang, L. and Ma, W., 2007, November. Improved real-valued clonal selection algorithm based on a novel mutation method. In 2007 International Symposium on Intelligent Signal Processing and Communication Systems (pp. 662-665). IEEE.

[179] Cutello, V., Nicosia, G. and Pavone, M., 2006, April. Real coded clonal selection algorithm for unconstrained global optimization using a hybrid inversely proportional hypermutation operator. In Proceedings of the 2006 ACM symposium on Applied computing (pp. 950-954).

[180] Bian, X. and Qiu, J., 2006, June. Adaptive clonal algorithm and its application for optimal PMU placement. In 2006 International Conference on Communications, Circuits and Systems (Vol. 3, pp. 2102-2106). IEEE.

[181] Kim, J. and Bentley, P.J., 2002, May. Towards an artificial immune system for network intrusion detection: an investigation of dynamic clonal selection. In Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No. 02TH8600) (Vol. 2, pp. 1015-1020). IEEE.

[182] Purbasari, A., Supriana, I., Santoso, O.S. and Mandala, R., 2013, July. Designing Artificial Immune System Based on Clonal Selection: Using Agent-Based Modeling Approach. In 2013 7th Asia Modelling Symposium (pp. 11-15). IEEE.

[183] Dai, H., Yang, Y., Li, H. and Li, C., 2014. Bi-direction quantum crossover-based clonal selection algorithm and its applications. Expert systems with applications, 41(16), pp.7248-7258.

[184] Peng, Y. and Lu, B.L., 2015. Hybrid learning clonal selection algorithm. Information Sciences, 296, pp.128-146.

[185] Zhao, T.S., Li, Z.Z., Mao, W.B. and Zhu, J.J., 2008, September. An automatic co-stimulation algorithm for LAN artificial immune systems. In 2008 IEEE Conference on Cybernetics and Intelligent Systems (pp. 478-481). IEEE.

[186] Matzinger, P., 2001. Essay 1: the Danger model in its historical context. Scandinavian journal of immunology, 54(1-2), pp.4-9.

[187] Matzinger, P., 1994. Tolerance, danger, and the extended family. Annual review of immunology, 12(1), pp.991-1045.

[188] Aickelin, U. and Cayzer, S., 2008. The danger theory and its application to artificial immune systems. (No. 0801.3549).

[189] Lebbe, M.A., Agbinya, J.I., Chaczko, Z. and Braun, R., 2008, May. Artificial immune system inspired danger modelling in Wireless Mesh

Networks. In 2008 International Conference on Computer and Communication Engineering (pp. 984-988). IEEE.

[190] Jim, L.E. and Gregory, M.A., 2016. A review of artificial immune system based security frameworks for MANET. International Journal of Communications, Network and System Sciences, 9(01), p.1.

[191] Behrozinia, S., Azmi, R., Keyvanpour, M.R. and Pishgoo, B., 2013, May. Biological inspired anomaly detection based on danger theory. In The 5th Conference on Information and Knowledge Technology (pp. 102-106). IEEE.

[192] M. Gill, D. Lindskog and P. Zavarsky, 2018. Profiling Network Traffic Behavior for the Purpose of Anomaly-Based Intrusion Detection. 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018 pp. 885-890. doi: 10.1109/TrustCom/BigDataSE.2018.00127.

[193] Kayacik, H.G., Zincir-Heywood, A.N. and Heywood, M.I., 2005, October. Selecting features for intrusion detection: A feature relevance analysis on KDD 99 intrusion detection datasets. In Proceedings of the third annual conference on privacy, security and trust (Vol. 94, pp. 1723-1722).

[194] Salem, M., Reißmann, S. and Buehler, U., 2014, February. Persistent dataset generation using real-time operative framework. In 2014 International Conference on Computing, Networking and Communications (ICNC) (pp. 1023-1027). IEEE.

[195] Thomas, C., Sharma, V. and Balakrishnan, N., 2008, March. Usefulness of DARPA dataset for intrusion detection system evaluation. In Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008 (Vol. 6973, p. 69730G). International Society for Optics and Photonics.

[196] Tavallaee, M., Bagheri, E., Lu, W. and Ghorbani, A.A., 2009, July. A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE symposium on computational intelligence for security and defense applications (pp. 1-6). IEEE.

[197] Haines, J.W., Lippmann, R.P., Fried, D.J., Zissman, M.A. and Tran, E., 2001. 1999 DARPA intrusion detection evaluation: Design and procedures. MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB.

[198] Sathya, S.S., Ramani, R.G. and Sivaselvi, K., 2011. Discriminant analysis based feature selection in kdd intrusion dataset. International Journal of computer applications, 31(11), pp.1-7.

[199] Kendall, K.K.R., 1999. A database of computer attacks for the evaluation of intrusion detection systems (Doctoral dissertation, Massachusetts Institute of Technology).

[200] Mahoney, M. and Chan, P., 2001. Packet header anomaly detection for identifying hostile network traffic. In Proceedings of the 2003 ACM symposium on applied computing, Melbourne, Florida (pp. 346-350).

[201] Yanbin, Z., Singh, S. and Silakari, S., 2015. Network intrusion detection system model based on artificial immune. International Journal of Security and Its Applications, 9(9), pp.359-370.

[202] Hofmeyr, S.A. and Forrest, S., 1999. An immunological model of distributed detection and its application to computer security (Doctoral dissertation, PhD thesis, University of New Mexico).

[203] Syahputra, R. and Soesanti, I., 2017, August. An artificial immune system algorithm approach for reconfiguring distribution network. In AIP Conference Proceedings (Vol. 1867, No. 1, p. 020017). AIP Publishing LLC.

[204] Revathi, S. and Malathi, A., 2013. A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection. International Journal of Engineering Research & Technology (IJERT), 2(12), pp.1848-1853.

[205] Dhanabal, L. and Shantharajah, S.P., 2015. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. International Journal of Advanced Research in Computer and Communication Engineering, 4(6), pp.446-452.

[206] Ernst, J., Hamed, T. and Kremer, S., 2018. A Survey and Comparison of Performance Evaluation in Intrusion Detection Systems. In Computer and Network Security Essentials (pp. 555-568). Springer, Cham.

[207] Shah, S.A.R. and Issac, B., 2017. Performance comparison of intrusion detection systems and application of machine learning to Snort system. Future Generation Computer Systems.

[208] Barani, F., 2014, February. A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system. In Intelligent Systems (ICIS), 2014 Iranian Conference on (pp. 1-6). IEEE.

[209] Shanmugam, B. and Idris, N.B., 2011. Hybrid intrusion detection systems (HIDS) using Fuzzy logic. Intrusion Detection Systems, pp.135-155.

[210] Yan, Q. and Yu, J., 2006, April. AINIDS: an immune-based network intrusion detection system. In Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2006 (Vol. 6241, p. 62410U). International Society for Optics and Photonics.

[211] Jinquan, Z., Xiaojie, L., Tao, L., Caiming, L., Lingxi, P. and Feixian, S., 2009. A self-adaptive negative selection algorithm used for anomaly detection. Progress in natural Science, 19(2), pp.261-266.

[212] Rojas-Gonzalez, I. and García-Gallardo, J., 2010. Bayesian network application on information security. IP Nacional, Ed., Research in Computing Science, 51, pp.87-98.

[213] Olusola, A.A., Oladele, A.S. and Abosede, D.O., 2010, October. Analysis of KDD'99 intrusion detection dataset for selection of relevance features. In Proceedings of the world congress on engineering and computer science (Vol. 1, pp. 20-22). WCECS.

[214] Mahoney, M.V., 2003. A machine learning approach to detecting attacks by identifying anomalies in network traffic.

[215] Ugtakhbayar, N., Battulga, D. and Sodbileg, S., 2012. Classification of artificial intelligence ids for smurf attack. arXiv preprint arXiv:1202.1886.

[216] Andhare, A. and Patil, A.B., 2012. Mitigating Denial-of-Service Attacks Using Genetic Approach. IOSR Journal of Engineering, 2(3), pp.468-472.

[217] Eddy, W.M., 2006. Defenses against TCP SYN flooding attacks. The Internet Protocol Journal, 9(4), pp.2-16.

[218] Lee, W., Stolfo, S.J. and Mok, K.W., 1999, August. Mining in a data-flow environment: Experience in network intrusion detection. In Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 114-124).

[219] Bhoria, P. and Garg, K., 2013. Determining feature set of DOS attacks. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), pp.875-878.

[220] Siddiqui, M.K. and Naahid, S., 2013. Analysis of KDD CUP 99 dataset using clustering based data mining. International Journal of Database Theory and Application, 6(5), pp.23-34.

[221] Nam, S.Y., Jurayev, S., Kim, S.S., Choi, K. and Choi, G.S., 2012. Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN. EURASIP Journal on Wireless Communications and Networking, 2012(1), p.89.

[222] Behboodian, N. and Razak, S.A., 2011, December. Arp poisoning attack detection and protection in wlan via client web browser. In International Conference on Emerging Trends in Computer and Image Processing (p. 20).

[223] Mittal, A., Shrivastava, A.K. and Manoria, M., 2011. A review of DDOS attack and its countermeasures in TCP based networks. International Journal of Computer Science and Engineering Survey, 2(4), p.177.

[224] Taylor, C. and Alves-Foss, J., 2000. Low cost network intrusion detection. Moscou: University of Idaho, p.15.

[225] Das, K.J., 2000. Attack development for intrusion detector evaluation (Doctoral dissertation, Massachusetts Institute of Technology).

[226] Choi, J., Choi, C., Ko, B., Choi, D. and Kim, P., 2013. Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment. J. Internet Serv. Inf. Secur., 3(3/4), pp.28-37.

[227] Choi, Y.S., Kim, I.K., Oh, J.T. and Jang, J.S., 2012, August. Aigg threshold based http get flooding attack detection. In International Workshop on Information Security Applications (pp. 270-284). Springer, Berlin, Heidelberg.

[228] Hudaib, A.A.Z., 2015. The Principles of Modern Attacks Analysis for Penetration Tester. International Journal of Computer Science and Security (IJCSS), 9(2), p.22.

[229] Northcutt, S. and Novak, J., 2002. Network intrusion detection. Sams Publishing.

[230] Low, C., 2001. Icmp attacks illustrated. SANS Institute URL: http://rr. sans. org/threats/ICMP attacks. php (12/11/2001).

[231] Win, M.T.M. and Khaing, K.T., 2013. Analyzing knowledge based feature selection to detect remote to local attacks. Int J Adv Res Comput Eng Technol, 2(5), pp.1762-1765.

[232] Lippmann, R.P., Fried, D.J., Graf, I., Haines, J.W., Kendall, K.R., McClung, D., Weber, D., Webster, S.E., Wyschogrod, D., Cunningham, R.K. and Zissman, M.A., 2000, January. Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. In Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00 (Vol. 2, pp. 12-26). IEEE.

[233] DeLooze, L.L. and Kalita, J., 2005. Applying soft computing techniques to intrusion detection. University of Colorado at Colorado Springs.

[234] Bsila, A., Gombault, S. and Belghith, A., 2007, March. Improving traffic transformation function to detect novel attacks. In 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (pp. 1-8).

[235] Akbar, S., Rao, K.N. and Chandulal, J.A., 2011. Implementing rule based genetic algorithm as a solution for intrusion detection system. International Journal of Computer Science and Network Security, 11(8), pp.138-144.

[236] Sabhnani, M. and Serpen, G., 2003, June. KDD Feature Set Complaint Heuristic Rules for R2L Attack Detection. In Security and Management (pp. 310-316).

[237] Mahoney, M.V. and Chan, P.K., 2002, July. Learning nonstationary models of normal network traffic for detecting novel attacks. In Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 376-385).

APPENDICES

Appendix A: Generated Rules in Reviewed Attacks (Examples)

Attack Type	#	Attack Name	Description	Generated Rules
Denial of Service (DOS)	1	Apache2	An attacker attacks the web server process by flooding it. An attacker sends a request with many http headers, if the server receives many of these requests it will slow down, and may eventually crash. The attack is most effective when all the headers are just the same [202].	protocol_type = tcp AND duration = xlong AND src_bytes = xxmany AND same_srv_rate = many AND dst_host_count = xmany AND dst_host_srv_count = xmany AND dst_host_same_srv_rate = xmany AND service = http AND srv_count = average AND traffic = many AND first_packet_flag = ACK-PSH AND system = apache AND header_size = many AND payload_length = long
	2	Smurf	An attacker floods the target network by sending ICMP ECHO REQUEST (ping) packets to a broadcast address (x.x.x.255) with the spoofed source address of the target. The target is then flooded with ECHO REPLY packets from multiple sources [216][217][218][219].	protocol_type = ICMP AND service = echo_i AND (count = average OR count = xmany) AND src_bytes = xmany AND flag = SF AND (srv_count = average OR srv_count = xmany) AND no_of_ICMP_Messgs = xmany AND is_broadcast= 1 AND dst_host_srv_count = xmany AND duration = vshort AND dst_host_count = xmany

	3	Neptune (SYN Flood)	The attackers send a large number of TCP SYN request packets with forged source IP addresses. This results in the server side consuming large amounts of resources in order to maintain a very large list of half open connections eventually leading to the server running out of resources and becoming unable to provide normal services. The attacker sends a stream of SYN packets to a port on a target machine [202][220] [221][222].	protocol_type = TCP AND serror_rate = many AND srv_serror_rate = many AND dst_host_srv_serror_rate = many AND dst_host_serror_rate = many AND dst_host_count = many AND count = average AND srv_count = vfew AND flag = S0 AND tcp_flag = SYN AND number_of_packets = many
	4	DoSNuke	DoSNuke is a Denial of Service attack that sends Out Of Band data (MSG_OOB) to port 139 (NetBIOS), crashing the NT victim (bluescreens the machine) crashes Windows by sending urgent data in a NetBIOS request [217].	service = netbios AND urgent >= 3 AND dst_host_count = many AND dst_host_srv_count = many AND same_srv_rate = many AND num_outbound_cmds > 2 AND system = NT (or any widows) AND tcp_flag = URG
	5	Ping of Death (POD)	Although the adverse effects of a Ping of Death could not be duplicated on any victim systems used in the 1998 DARPA evaluation, it has been widely reported that some systems will react in an unpredictable fashion when receiving oversized IP packets [16][216][217][222].	protocol_type = ICMP AND service = ICMP AND src_bytes = xmany AND same_srv_rate = many AND dst_host_same_srv_rate = many AND dst_host_same_src_port_rate = many AND wrong_fragment > 0 AND duration = average AND average_packet_size = xxmany (> 65,536)

	6	Back	In this denial of service attack against the Apache web server, an attacker submits requests with URL's containing many frontslashes. As the server tries to process these requests it will slow down and becomes unable to process other requests. A request with 100 frontslashes in the URL would be highly irregular on most systems [202][203][222][223].	src_bytes = xxmany AND des_bytes = xmany AND same_srv_rate = many AND dst_host_same_srv_rate = xmany AND duration = short AND logged_in = 1 AND num_compromised > 0 AND dst_host_count = average AND Protocol_type = TCP AND service = http AND system = Apache AND number_of_packets = many AND payload_length = long
	7	Teardrop	The teardrop exploit is a denial of service attack that exploits a flaw in the implementation of older TCP/IP stacks. Some implementations of the IP fragmentation re-assembly code on these platforms does not properly handle overlapping IP fragments [202][216][217][223].	wrong_fragment >= 3 AND protocol_type = UDP AND count = few AND srv_count = few AND same_srv_rate = many AND dst_host_count = xmany AND dst_host_srv_count = average AND service = private AND dst_host_same_srv_rate = few AND duration = average
	8	Tcpreset	TCP Reset is a denial of service attack that disrupts TCP connections made to the victim machine. The attacker listens for tcp connections to the victim, and sends a spoofed tcp RESET packet to the victim, thus causing the victim to inadvertently terminate the TCP connection [217].	protocol_type = TCP AND flag = RTSO AND tcp_flag = RST AND is_hot_login = 1 AND average_packet_size = small AND first_packet_flag = ACK-PSH
	9	CrashIIS	CrashIIS is a Denial of Service attack against the NT IIS webserver. The attacker sends a malformed GET request via telnet to port 80 on the NT victim. The command "GET ../.."	service = http AND duration = short AND flag = S1 AND

			crashes the web server and sometimes crashes the ftp and gopher daemons as well, because they are part of IIS. Crashiis attack sent only seven and five packet s to the victim IPs in two separated connections [202][217][224][225]	protocol_type = TCP AND number_of_packets = small AND average_packet_size = vsmall AND system = NT IIS
	10	MailBomb	A Mailbomb is an attack in which the attacker sends many messages to a server, overflowing that server's mail queue and possible causing system failure. Auser is flooded with mail messages, a typical attack would send more than 10,000 one kilobyte messages (10 megabytes of total data) to a single user [201][202][217][226][227].	protocol_type = tcp AND duration = short AND service = SMTP AND src_bytes = xxmany AND dest_bytes = few AND same_srv_rate = many AND dst_host_count = many AND dst_host_rerror_rate = many AND srv_count = xmany AND dst_host_srv_count = few
	11	Selfping	Selfping is a denial of service attack which allows a user without administrative privileges to remotely reboot a machine with a single ping command. The ping command broadcasts echo_request packets using the localhost as the multicast interface [203][217][228].	protocol_type = ICMP AND srv_diff_host_rate = many AND service = Echo_Request AND src_bytes = vfew AND srv_count = many AND same_srv_rate = many AND system = solaris
	12	Processtable	An attacker opens a large number of connections to a service such as finger, POP3 or IMAP until the number of processes exceeds the limit. At this point no new processes can be created until the target is rebooted. For most machines, hundreds of connections to the finger port would certainly constitute unusual behavior [217].	duration = xxlong AND protocol_type = TCP AND same_srv_rate = many AND srv_count = many AND [service = port 79 AND] dst_host_count = xmany AND dst_host_srv_count = average AND dst_host_srv_error_rate = average
	13	http GET flooding attack	An HTTP flood is an attack method used by hackers to attack web servers and applications. It consists of seemingly legitimate session-based sets of HTTP GET or POST requests	Protocol_type = TCP AND Service = http AND dst_host_count = many AND

			sent to a target web server. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service condition. Such requests are often sent in masse by means of a botnet, increasing the attack's overall power [229][230].	average_packet_size = small AND count = many AND srv_count = many
	14	SSHprocesstable	SSH Processtable is similar to the processtable attack in that the goal of the attacker is to cause sshd daemon on the victim to fork so many children that the victim can spawn no more processes. This is due to a kernel limit on the number of processes that the OS will allow.	service = ssh AND count = many AND srv_count = many AND dst_host_count = xmany AND dst_host_srv_count = many
	15	WinFreeze	WinFreeze use false ICMP redirect messages to attempt to convince a host to use itself as the optimal router. Obviously, any packet which tells a device to route everything to itself, should be considered highly abnormal. Cause susceptible Windows host to attack Itself (self - mutilation) [195] [231][232].	Protocol_type=ICMP AND (System=windows AND Count = many AND srv_count=many AND dst_host_count = many AND dst_host_srv_count = many) OR land =1
	16	Xmax scan	Xmax scan sends TCP frame to remote device with TCP flags URG, ACH, SYN and FIN sets as ON.	protocol_type = TCP AND TCP_flag = URG AND TCP_flag = ACK AND TCP_flag =SYN AND TCP_flag = FIN AND src_bytes = small system <> Windows
	17	Loki (and Loki2)	Uses ICMP and UDP protocol tunnelling to obtain a reverse shell from an attacked system. In such an attack, the traffic that is being exchanged between the Loki client & Loki server is almost covert as there are no listening ports opened on the victim machine and even the traffic could be encrypted with an encryption algorithm like Blowfish or DH for additional covertness [233].	root_shell=1 AND logged_in =1 AND num_file_creations >= 1 AND src_bytes = many AND protocol_type=ICMP AND duration = long
Probes	18	IPsweep	An Ipsweep attack is a surveillance sweep to determine which hosts are listening on a network. This information is useful to	service = eco_i AND (protocol_type = ICMP OR TCP)

			an attacker in staging attacks and searching for vulnerable machines [202][216][223].	AND (dst_host_srv_diff_host_rate = many Or average) AND count = many AND rerror_rate = many AND srv_error_rate = many AND dst_host_srv_count = average AND dst_host_same_srv_rate = many AND dst_host_same_src_port_rate = many AND same_srv_rate = many AND no_of_packets = small AND same_source_IP = 1
	19	QueSO	QueSO is a probe used to determine the type and operating system of a machine that exists at a certain IP address. QueSO sends a series of seven TCP packets to a particular port of a machine. Many of the packets QueSO sends do not have specified responses in the TCP RFC. The first 4 packets are normal requests to open and close a connection, the remaining 3 packets are abnormal requests looking for anomolous behavoir to help classify the machine and OS [203][217][228].	Protocol_type = TCP AND (FLAG = SH OR SHR) AND no_of_packets = small (= 7) AND TCP_flag = FIN AND TCP_flag = SYN+FIN AND duration = long AND count = many
	20	Saint	SAINT is the Security Administrator's Integrated Network Tool. In its simplest mode, it gathers as much information about remote hosts and networks as possible by examining such network services as finger, NFS, NIS, ftp and tftp, rexd, statd, and other services [201][202].	diff_srv_rate = many AND rerror_rate = many AND dst_host_count = many AND dst_host_rerror_rate = many AND dst_host_srv_error_rate = many AND flag = REJ AND srv_error_rate = many
	21	Satan	SATAN is an early predecessor of the SAINT scanning program described in the last section. While SAINT and SATAN are quite similar in purpose and design, the particular	diff_srv_rate =many AND protocol_type = UDP AND dst_host_srv_count = average AND

			vulnerabilities that each tools checks for are slightly different [202][216][217].	dst_host_srv_error_rate = many AND dst_host_count = many AND flag = REJ AND rerror_rate = many AND average_packet_size = big
	22	MScan	Mscan is a probing tool that uses both DNS zone transfers and/or brute force scanning of IP addresses to locate machines, and test them for vulnerabilities.	duration = short AND diff_srv_rate = many AND protocol = tcp AND count = Vfew AND srv_count = Vfew AND srv_diff_host_rate = xmany AND dst_host_srv_error_rate = many AND rerror_rate = many AND srv_error_rate = average
	23	NTinfoScan	NTInfoScan is a NetBIOS based security scanner. It scans the NT victim to obtain share information, the names of all the users, services running, and other information. The results are saved in an html file named .html where victim is the victim's hostname [217].	duration = long AND service = ftp AND flag = RSTOS AND tcp_flag = RST AND TTL = 126 AND system = NT
	24	Portsweep	Surveillance sweep through many ports to determine which services are supported on a single host. This attack is focused in one host [16][202][217].	dst_host_count = many AND count = few AND diff_srv_rate = many AND srv_diff_host_rate = many AND protocol_type = (TCP OR ICMP) AND rerror_rate = many AND duration = long AND dst_host_same_srv_rate = average AND

				dst_host_diff_srv_rate = average AND srv_error_rate = many AND service = (ports 19 (chargen) OR port 143)
	25	Nmap	Nmap is a general-purpose tool for performing network scans. Nmap supports many different types of port scan options include SYN, FIN and ACK scanning with both TCP and UDP, as well as ICMP (Ping) scanning. The Nmap program also allows a user to specify which ports to scan, how much time to wait between each port, and whether the ports should be scanned sequentially or in a random order.	diff_srv_rate = many AND count = few AND srv_count = few AND Duration = long AND same_srv_rate = xmany AND dst_host_count = many AND dst_host_same_srv_rate = many AND dst_host_same_src_port_rate = many
Remote to Local Attacks (R2L)	26	Dictionary	An attacker tries to gain access to some machine by making repeated guesses at possible usernames and passwords. It is an attack of password guessing using dictionary words [202] [203][234].	num_failed_logins >= 3 AND dst_host_count = many AND count = many AND srv_count = many AND dst_host_srv_count = many AND (services = telnet or ftp or pop or rlogin or imap) AND logged_in > 0
	27	SendMail	The Sendmail attack exploits a buffer overflow in version 8.8.3 of sendmail and allows a remote attacker to execute commands with superuser privileges. By sending a carefully crafted email message to a system running a vulnerable version of sendmail, intruders can force sendmail to execute arbitrary commands with root privilege [202].	service = SMTP AND src_bytes = xxmany AND dest_bytes =average AND su_attempted =1 AND num_failed_logins >=2 AND is_hot_login=1 AND same_srv_rate = many AND dst_host_count = many AND system = linux

	28	Imap	The Imap attack exploits a buffer overflow in the Imap server of Redhat Linux 4.2 that allows remote attackers to execute arbitrary instructions with root privileges [202][203] [216][223].	service = imap AND is_hot_login = 1 AND dst_host_srv_count = many AND same_srv_rate = many AND dst_host_same_srv_rate = many AND protocol_type = TCP AND system = Linux AND hot > 1 AND srv_count = average AND root_shell = 1 AND duration = average
	29	NcFTP	Ncftp is an ascii UI ftp program for linux. This attack exploits one of the popular features of the program: the ability to get subdirectories recursively. Five instances of this attack were run against the Linux victim. Attacks against Linux can only be seen in the sniffer data because there is no host-based auditing [203][217][228].	service = ftp AND count = many AND same_srv_rate = many AND hot > 2 AND logged_in = 1 AND system = linux
	30	Xlock	In the Xlock attack, a remote attacker gains local access by fooling a legitimate user who has left their X console unprotected, into revealing their password. The xlock attack scans for open X servers, then displays a fake screensaver which prompts the user to enter a password, which is then captured [201][202][217].	duration = average AND protocol_type = tcp AND src_bytes = xxmany AND dest_bytes = xmany AND same_srv_rate = many AND dst_host_count = many AND logged_in = 1 AND count = many AND dst_host_same_srv_rate = many
	31	Xsnoop	In the Xsnoop attack, an attacker watches the keystrokes processed by an unprotected X server to try to gain information that can be used gain local access the victim system. An attacker can monitor keystrokes on the X server of a user who has left their X display open [200][201][202][235].	duration = short AND protocol_type = tcp AND src_bytes = xxmany AND dest_bytes = xmany AND same_srv_rate = many AND

				dst_host_count = many AND count = many AND num_shells >=2
	32	Guest	The Guest attack is a variant of the Dictionary attack. On badly configured systems, guest accounts are often left with no password or with an easy to guess password. Because most operating systems ship with the guest account activated by default, this is one of the first and simplest vulnerabilities an attacker will attempt to exploit [202][217].	is_guest_login = 1 AND num_failed_logins >2 AND dst_host_count = many AND count = many AND duration = short AND service = telnet OR rlogin
	33	Netbus	NetBus is a Remote to Local attack. The attacker uses a trojan program to install and run the Netbus server on the victim machine. Once Netbus is running, it acts as a backdoor. The attacker can then remotely access the machine using the Netbus client. The Netbus client can also be used as a probe attack to scan IP addresses for NetBus servers. When the attacker uses the netbus client to access the victim, it creates network traffic that is easy to identify [200][217].	dst_host_count = many AND protocol_type = TCP AND (Port = 12345 OR = 12346 OR = 20034) AND count = many AND flag = S1 AND logged_in = 1 AND system = NT AND payload_length = long
	34	FTPWrite	The Ftp-write attack is a Remote to Local User attack that takes advantage of a common anonymous ftp misconfiguration [200][217].	service = (FTP OR ftp_data OR printer (port 515)) AND same_srv_rate = many AND dst_host_count = many AND src_bytes = many AND protocol_type = TCP AND num_file_creations >1 AND urgent >1
	35	Phf	The Phf attack abuses a badly written CGI script to execute commands with the privilege level of the http server. Any CGI program which relies on the CGI function escape_shell_cmd() to prevent exploitation of shell-based library calls may be vulnerable to attack. In particular, this vulnerability is manifested by the "phf" program that is distributed with the example code for the Apache web server [217][223][236].	protocol_type = TCP AND service = http AND dest_bytes = xmany AND same_srv_rate = many AND dst_host_count = many AND dst_host_srv_count = many AND dst_host_same_srv_rate = many

				AND logged_in = 1 AND root_shell = 1 AND hot > 1 AND payload_length = short
	36	Spy	The spy is an information collector who comes back to a compromised machine several times to collect information. A spy might be looking for confidential data files or reading user's personal mail. A spy will take steps to minimize the possibility of detection [202].	duration = long AND protocol_type = TCP AND src_bytes = many AND dest_bytes = xmany AND dst_host_count = many AND dst_host_srv_serror_rate = many AND same_srv_rate = many AND service = Telnet AND Flag = SF
	37	SNMP GET Attack	An attacker who has guessed the SNMP community password of a router will then be able to monitor the traffic levels on that router, and may be able to issue commands to the router to change default routes or allow connections from a previously forbidden host or network [202][234][235][237].	Protocol_type = udp AND service = private AND flag = sf AND src_bytes = few AND dest_bytes = few AND same_srv_rate = many AND dst_host_count = many AND dst_host_srv_count = many AND dst_host_same_srv_rate = many AND System = router
	38	SNMP Guess Attack	In the case of the snmpguess attack, the attacker sends infinity of SNMP request with various community name and the victim replies for each one, by sending an empty SNMP message. Each couple of request reply is considered as a SNMP connection independently from the others. To differentiate the SNMP attack traffic from that normal we used the two attributes "num_failed_login" and "logged_in" which	protocol_type = udp AND duration = short AND num_failed_logins > 1 AND logged_in = 1 AND service = private AND srv_error_rate = many AND dst_host_count = many AND dst_host_srv_count = many AND

			belong to the 41 attributes of the transformation function [234][237].	dst_host_same_srv_rate = many AND no_of_packets = many
	39	Named	The Named attack exploits a buffer overflow in BIND. An improperly or maliciously formatted inverse query on a TCP stream destined for the named service can crash the named server or allow an attacker to gain root privileges [200] [202][217][235][236].	protocol_type = tcp AND service = DNS AND is_hot_login = 1 AND root_shell = 1 AND dst_host_count = many AND dst_host_srv_count = many AND dst_host_same_srv_rate = many AND duration = short AND (src_bytes = many OR src_bytes = xxmany) AND same_srv_rate = many AND system = Linux
	40	Guess Password	Guess password (GPW) attack uses a brute force technique to discover the password of a local account by trying every word in a “password dictionary”, therefore opening many connections to the victim. Any service requiring password is vulnerable to this kind of attack like FTP or Telnet [16][217][234].	dst_host_count = many AND protocol = TCP AND num_failed_logins > 0 AND rerror_rate = many AND count = many AND dst_host_rerror_rate = many AND dst_host_same_srv_rate = many AND dst_host_srv_error_rate = many AND src_bytes = few AND dest_bytes = few AND duration = average AND srv_error_rate = many AND same_srv_rate = many AND service = (FTP OR Telnet OR POP3 OR IMAP OR SSH)

	41	Multihop	An attacker first breaks into one inside machine, and then uses this inside machine for further attacks on the rest of the network [202][223].	dest_bytes = many AND src_bytes = many AND protocol_type = TCP AND same_srv_rate = many AND dst_host_same_srv_rate =many AND dst_host_same_src_port_rate = many AND hot > 2 AND num_compromised > 1 AND duration = long
	42	WarezMaster	Uploading illegal software from a local anonymous FTP server. Warezmaster exploits a system bug associated with a file transfer protocol (FTP) server. Normally, guest users are never allowed write permissions on an FTP server. Hence they can never upload files on the server [201][216][223] [238][239].	dest_bytes = xmany AND duration = long AND same_srv_rate = many AND dst_host_same_srv_rate = many AND dst_host_same_src_port_rate = many AND protocol_type = TCP AND srvice = FTP_Data AND dst_host_srv_count = average AND src_bytes = xmany
	43	WarezClient	Downloading illegal software from a local anonymous FTP server [217][238][239].	protocol_type = TCP AND (Service = FTP Or FTP_Data) AND duration = short AND (logged_in = 1 OR is_guest_login = 1) AND hot > 3 AND Src_bytes = many AND num_compromised = many AND same_srv_rate = many AND dst_host_same_srv_rate = many AND dst_host_same_src_port_rate = many

User to Root Attacks (U2R)	44	Sechole	The attacker (a regular user) ftps to the victim and uploads test.exe and testfile.dll (filenames were chosen to be stealthy). The attacker then telnets to the victim and runs test.exe [200] [203][217].	num_file_creations > 2 AND num_shells > 1 AND hot > 2 AND protocol_type = TCP AND service = (FTP OR Telnet) AND sysrem = Windows NT
	45	Xterm	The Xterm attack exploits a buffer overflow in the Xaw library distributed with Redhat Linux 5.0 (as well as other operating) and allows an attacker to execute arbitrary instructions with root privilege. Problems exist in both the xterm program and the Xaw library that allow user supplied data to cause buffer overflows in both the xterm program and any program that uses the Xaw library.	logged_in = 1 AND num_root > 2 AND is_hot_login = 1 AND num_file_creations > 2 AND hot > 1 AND num_compromised >2 AND num_shells > 1 AND dst_host_rerror_rate =many AND rerror_rate = many AND duration = average AND src_bytes = xmany AND dest_bytes = xmany AND same_srv_rate = many
	46	Eject	The Eject attack exploits a buffer overflow is the 'eject' binary distributed with Solaris 2.5. In Solaris 2.5, removable media devices that do not have an eject button or removable media devices that are managed by Volume Management use the eject program [22][74][200][202][217][228][235].	is_hot_login = 1 AND service = FTP AND num_root > 2 AND root_shell = 1 AND su_attempted = 1 AND first_packet_flag = ACK-PSH AND system = unix
	47	Ps	The Ps attack takes advantage of a race condition in the version of 'ps' distributed with Solaris 2.5 and allows an attacker to execute arbitrary code with root privilege (sh-79). The ps attack uses a buffer overflow is to exploit a race condition in the ps program. Because of poor temporary file management in the ps program, this buffer overflow can hijack the ps	is_hot_login = 1 AND num_file_creations > 1 AND hot > 1 AND logged_in = 1 AND protocol_type = tcp AND src_bytes = few AND

			program when it is given an illegal option [74][202][203][228].	service = FTP OR Telnet AND dest_bytes = many AND same_srv_rate = many AND dst_host_count = average AND duration = short AND dst_host_srv_count =averge AND system = solaris AND header_size = many
	48	Perl	The Perl attack is a User to Root attack that exploits a bug in some Perl implementations. Suidperl is a version of Perl that supports saved set-user-ID and set-group-ID scripts [22][200] [202][203][223].	root_shell = 1 AND protocol_type = TCP AND service = Telnet AND dest_bytes = many AND same_srv_rate = many AND num_root > 1 AND num_failed_logins > 1 AND diff_srv_rate = many AND dst_host_count = many AND is_hot_login = 1 AND system = Linux
	49	Yaga	Yaga is a User-to-Root attack. It adds the attacker to the Domain Admins group by hacking the registry. The attacker edits the victim's registry so that the next time a system service crashes on the victim, the attacker is added to the Domain Admins group. To setup the attack, the attacker must put onto the victim machine a file with the registry edit information [22][200][203][240].	hot > 1 AND num_root > 1 AND num_file_creations >= 2 AND service = http AND duration = short AND number_of_packets = small AND aveargе_packet_size = xsmall
	50	Fdformat	The Fdformat attack exploits a buffer overflow is the 'fdformat' program distributed with Solaris 2.5. The fdformat program formats diskettes and PCMCIA memory cards. The program also uses the same volume management library, libvolmgt.so.1, and is exposed to the same vulnerability as the eject program [22] [74][200][202][235].	is_hot_login = 1 AND service = FTP AND root_shell = 1 AND hot >1 AND root_shell = 1 AND num_root >1 AND system = Solaris AND

				header_size = many
	51	Casesen	CaseSen is a User to Root attack that exploits the case sensitivity of the NT object directory. The attacker ftps three attack files to the victim: soundedt.exe, editwavs.exe, psxss.exe (the names of the files were chosen to make the attack more stealthy). The attacker then telnets to the victim and runs soundedt.exe [203][217].	service = (FTP OR Telnet) AND num_file_creations > 2 AND is_hot_login = 1 AND duration = short AND num_root = many AND hot >2 AND system = NT
	52	Loadmodule	The Loadmodule attack is a User to Root attack against SunOS 4.1 systems that use the xnews window system. The loadmodule program within SunOS 4.1.x is used by the xnews window system server to load two dynamically loadable kernel drivers into the currently running system and to create special devices in the /dev directory to use those modules. Because of a bug in the way the loadmodule program sanitizes its environment, unauthorized users can gain root access on the local machine [200][202][203][216][217][223][228][235][236].	is_hot_login = 1 AND Hot > 2 AND duration = average AND protocol_type = TCP AND dest_bytes = many AND src_bytes = average AND same_srv_rate = many AND dst_host_same_src_port_rate = many AND service = telnet OR FTP OR FTP_Data AND root_shell = 1 AND system = SunOS
	53	SQLAttack	Sqlattack is a version of perl that is run by connecting to the SQL server on a machine and escaping to a shell to run the perl attack. An attacker established a telnet connection with the SQL server of the victim machine. After executing a few normal SQL queries, the attacker escaped to a shell which he used to launch a perl attack [200][217][228].	root_shell = 1 AND is_hot_login = 1 AND num_file_creations > 2 AND num_root > 2AND hot > 1 AND same_srv_rate = many AND dst_host_count = many AND dst_host_srv_count = average AND protocol = tcp AND service = telnet AND src_bytes = many AND dest_bytes = xmany AND system = Linux

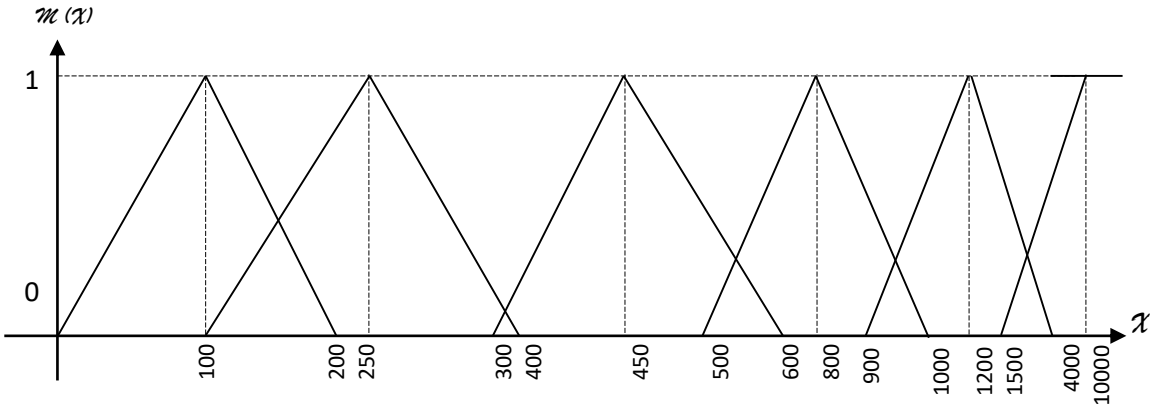
	54	Rootkit	A rootkit is a collection of programs that are intended to help a hacker maintain access to a machine once it has been compromised. A typical rootkit consists of a sniffer, versions of login, su, and other programs with backdoors which allow for access, and new versions of ps, netstat, and ls that hide the fact that a sniffer is running and hide files in certain directories [202] [216][223].	protocol_type = (TCP OR UDP) AND same_srv_rate = many AND flag = SF AND (dst_host_count = many) AND (duration = long) AND srv_count =many
	55	Ffbconfig	The Ffbconfig attack exploits a buffer overflow is the 'ffbconfig' program distributed with Solaris 2.5. The ffbconfig program configures the Creator Fast Frame Buffer (FFB) Graphics Accelerator, which is part of the FFB Configuration Software Package, SUNWffbcf. This software is used when the FFB Graphics accelerator card is installed. Due to insufficient bounds checking on arguments, it is possible to overwrite the internal stack space of the ffbconfig program [200][202][203][228][235].	num_root > 1 AND hot > 1AND is_hot_login = 1 AND root_shell = 1 AND duration = average AND system = Solaris
	56	Buffer overflow	Buffer overflow errors are characterized by the overwriting of memory fragments of the process, which should have never been modified intentionally or unintentionally [216][223].	protocol_type = TCP AND dest_bytes = xmany AND same_srv_rate = many AND dst_host_same_srv_rate = many AND dst_host_same_src_port_rate = many AND duration = long AND logged_in = 1

Appendix B: Fuzzy Sets for the KDD'99 Features:

1- Duration [237]

Scale: 0 – 22000

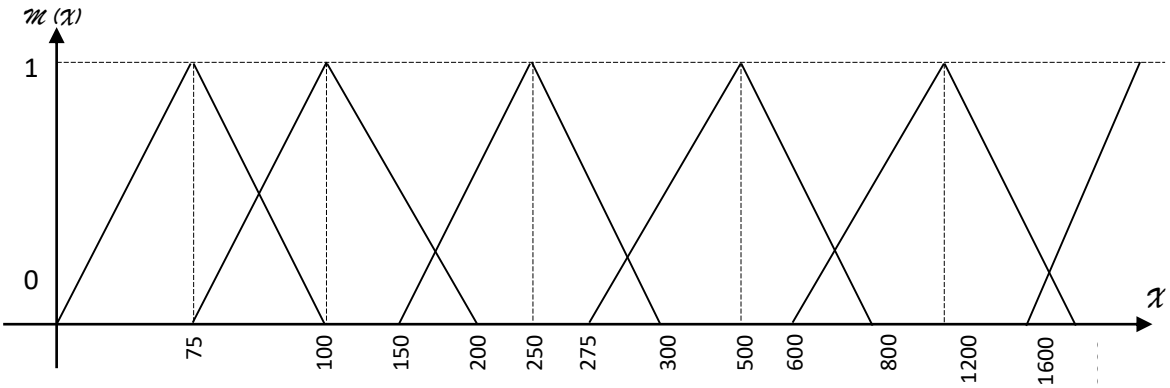
FSs: short<0,100,200>; average<100,250,400>; long<300,450,600>; vlong<500,800,1000>; xlong<900,1200,4000>; xxlong<1500,10000,…>



2- src_bytes

Scale: 0 – 2000

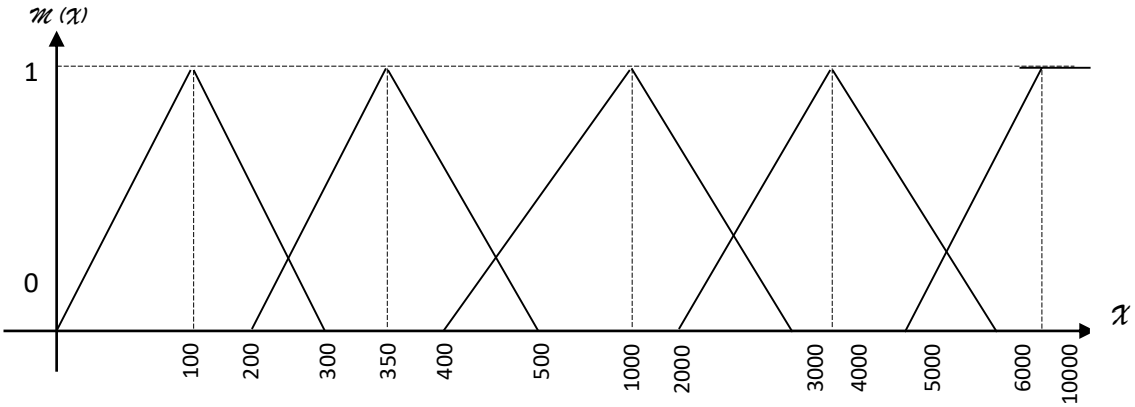
FSs: vfew<0,75,100>; few<75,100,200>; average<150,250,300>; many<275,500,800>; xmany<600,1200,2000>; xxmany<1600,3000,….>



3- dest_bytes

Scale: 0 -10000

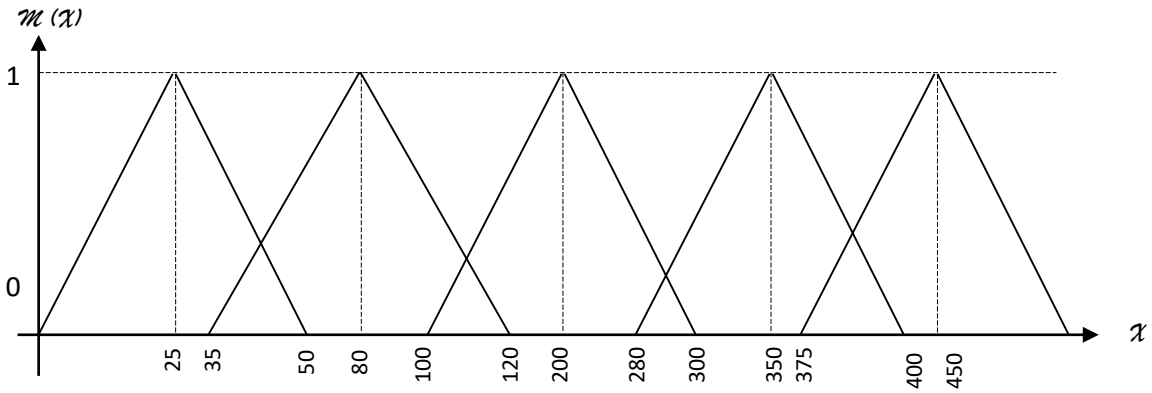
FSs: vfew<0,100,300>; few<200,350,500>; average<400,1000,3000>; many<2000,4000,6000>; xmany<5000,10000,…>



4- count

Scale: 0 – 520

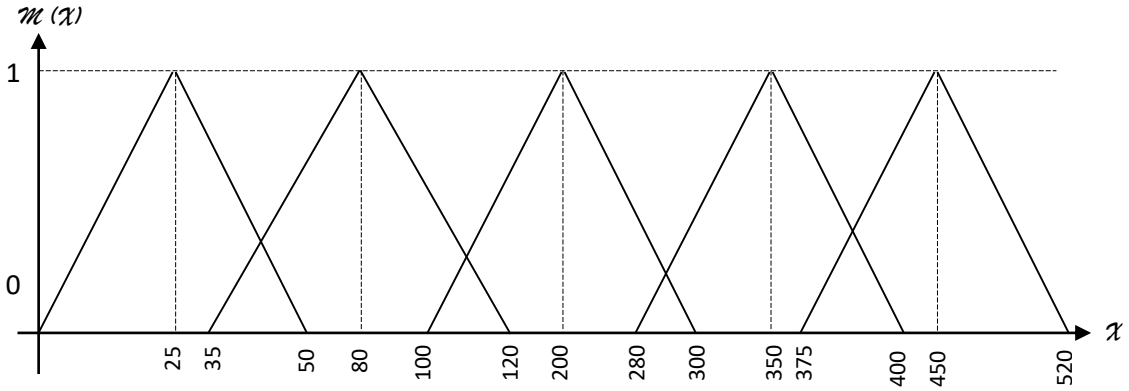
FSs: vfew<0,25,50>;few<35,80,120>;average<100,200,300>;
many<280,350,400>; xmany<375,450,520>



5- srv_count

Scale: 0 – 520

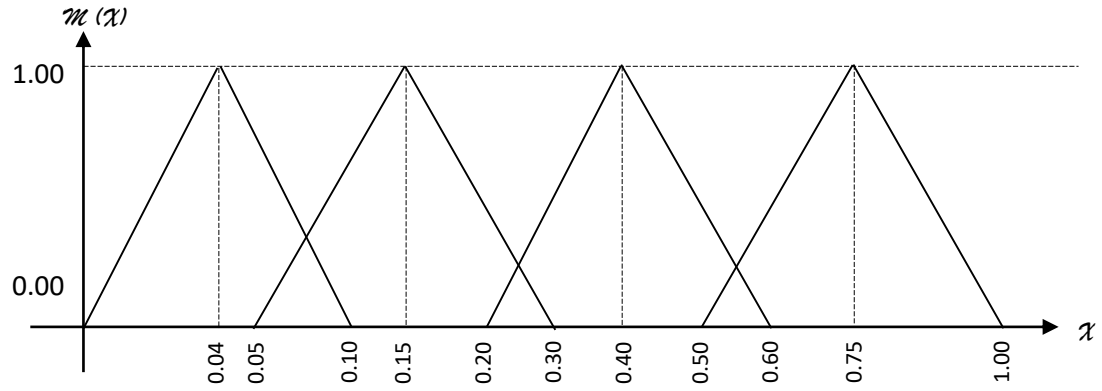
FSs: vfew<0,25,50>;few<35,80,120>;average<100,200,300>;
many<280,350,400>; xmany<375,450,520>



6- serror_rate

Scale: 0.00 – 1.00

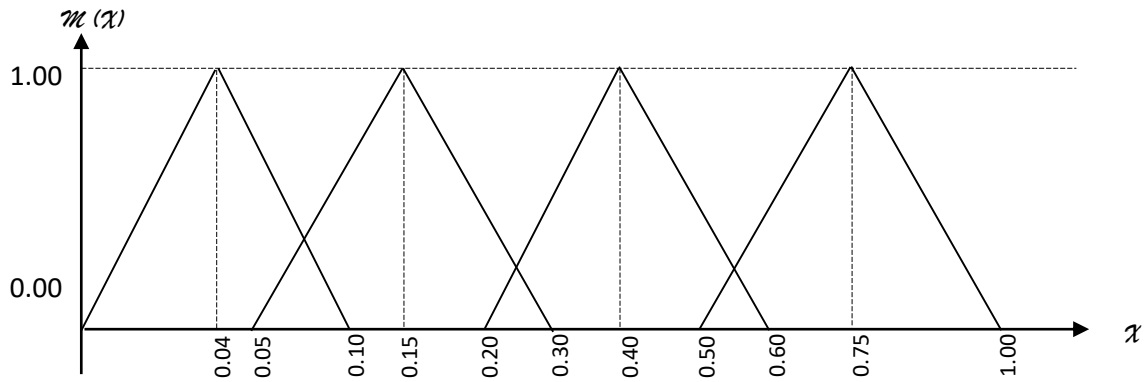
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>;
many<0.50,0.75,1.00>



7- srv_serror_rate

Scale: 0.00 – 1.00

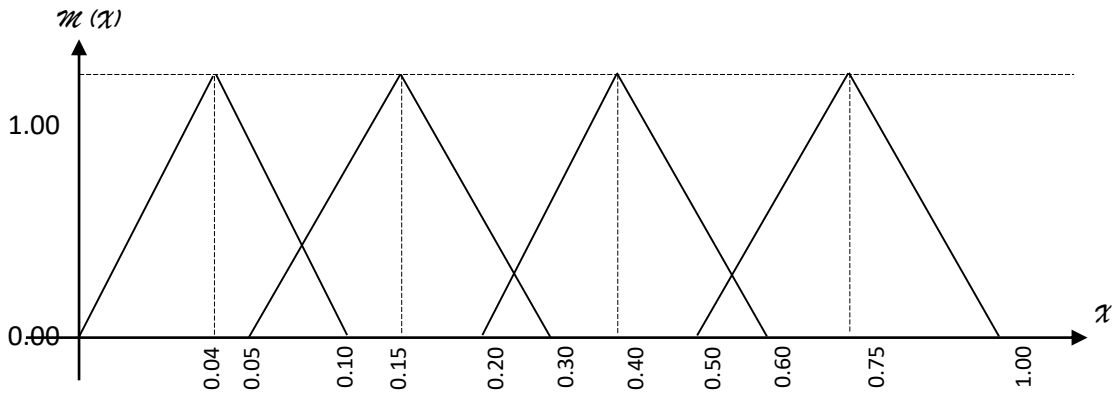
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



8- rerror_rate

Scale: 0.00 – 1.00

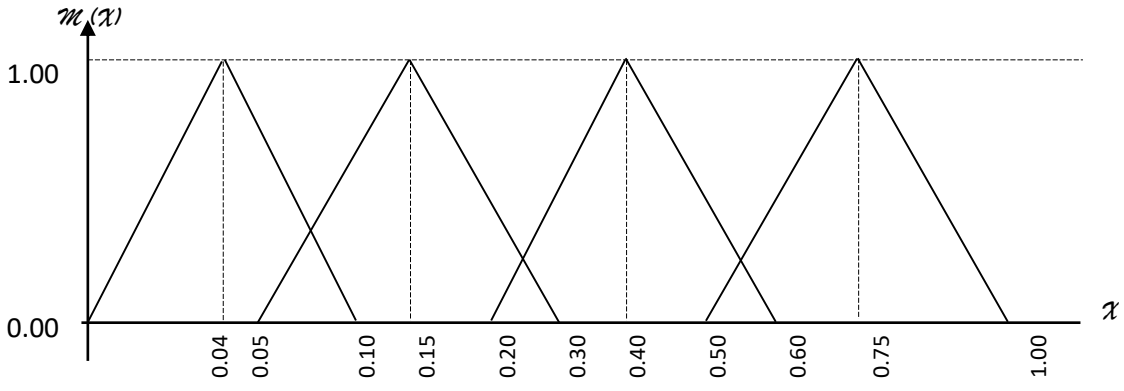
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



9- srv_error_rate

Scale: 0.00 – 1.00

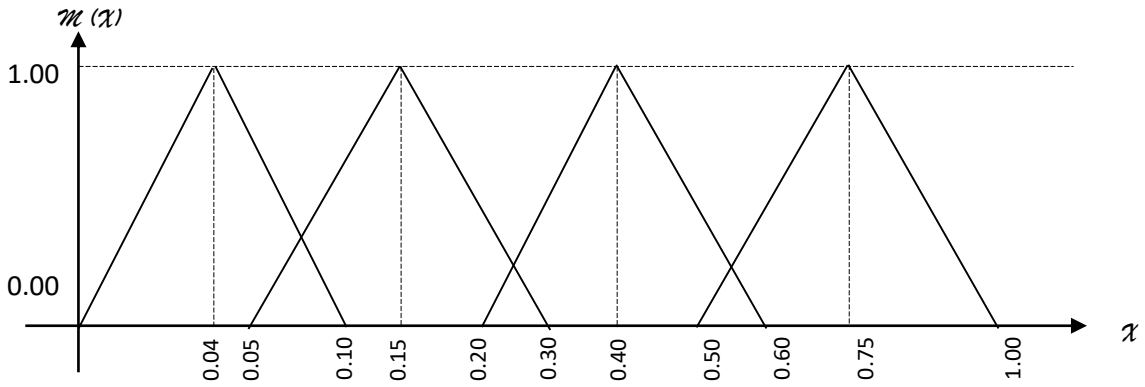
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



10- same_srv_rate

Scale: 0.00 – 1.00

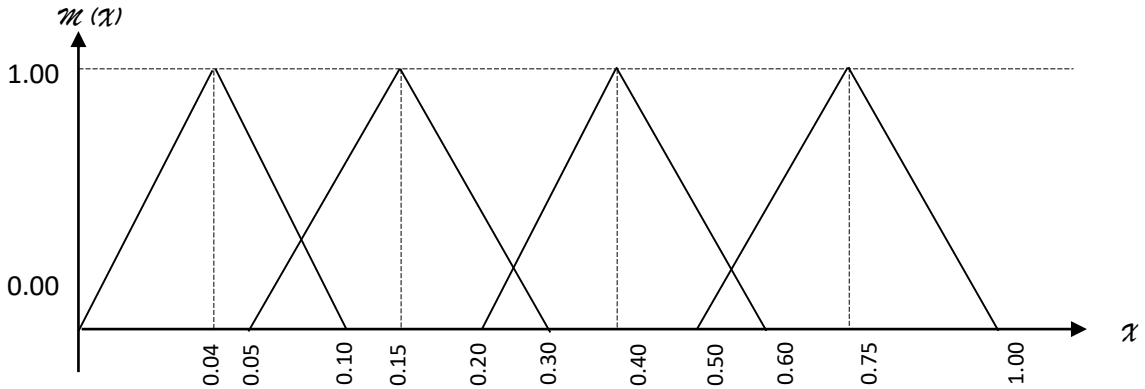
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



11- diff_srv_rate

Scale: 0.00 – 1.00

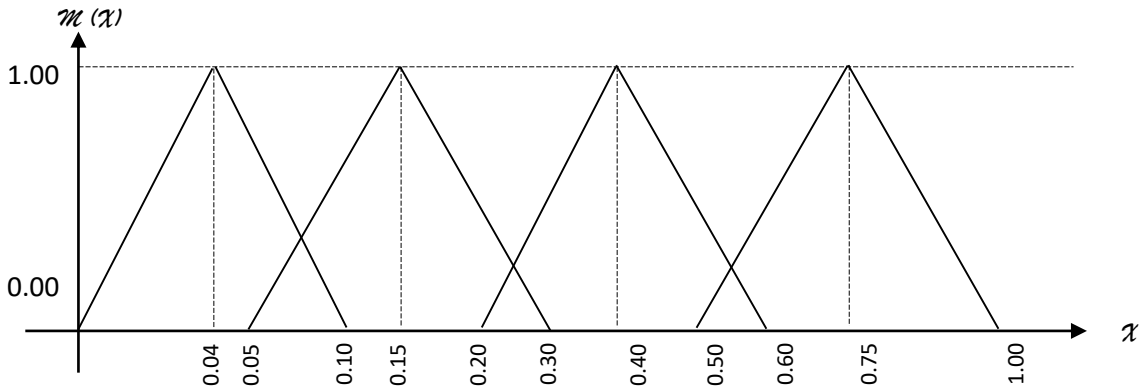
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



12- srv_diff_host_rate

Scale: 0.00 – 1.00

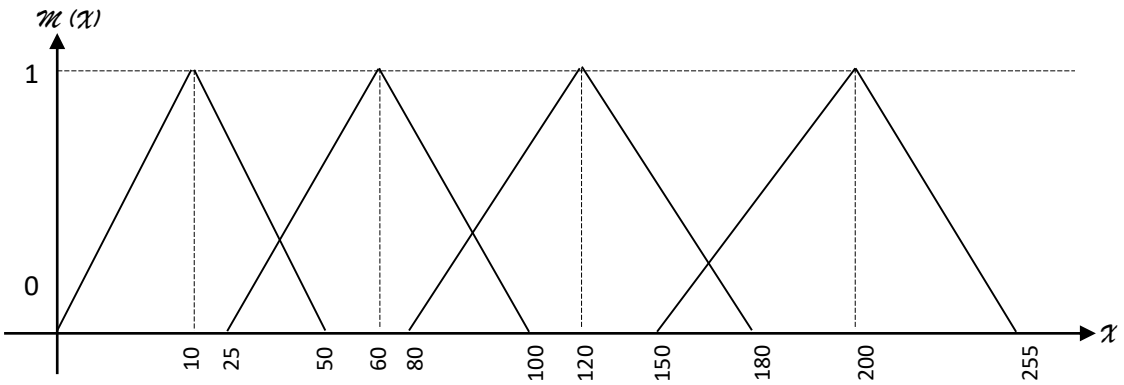
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



13- dst_host_count

Scale: 0 – 255

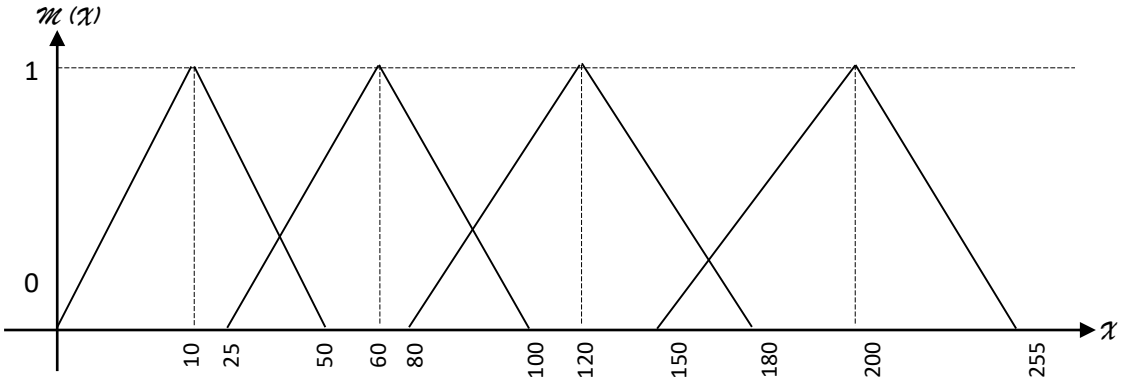
FSs: few<0,10,50>; average<25,60,100>; many<80,120,180>; xmany<150,200,255>



14- dst_host_srv_count

Scale: 0 – 255

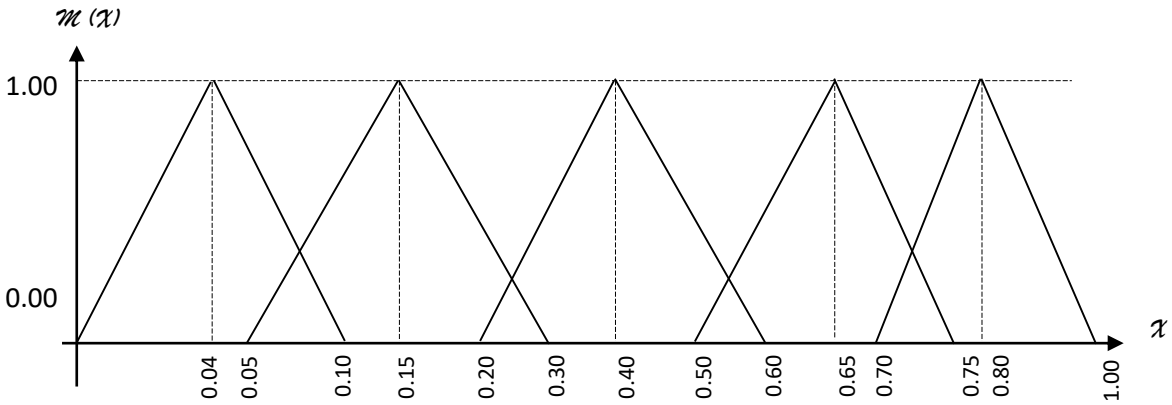
FSs: few<0,10,50>; average<25,60,100>; many<80,120,180>; xmany<150,200,255>



15- dst_host_same_srv_rate

Scale: 0.00 – 1.00

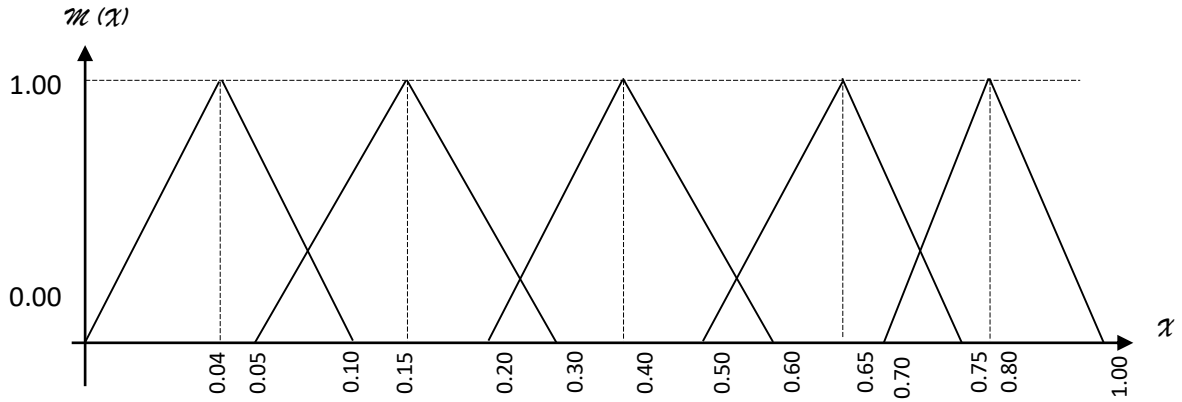
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.65,0.75>; xmany<0.70,0.80,1.00>



16- dst_host_diff_srv_rate

Scale: 0.00 – 1.00

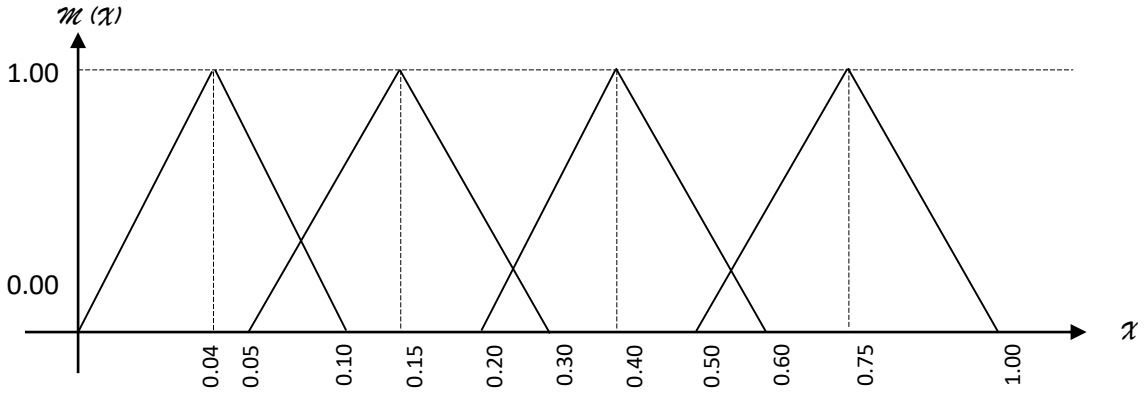
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.65,0.75>; xmany<0.70,0.80,1.00>



17- dst_host_same_src_port_rate

Scale: 0.00 – 1.00

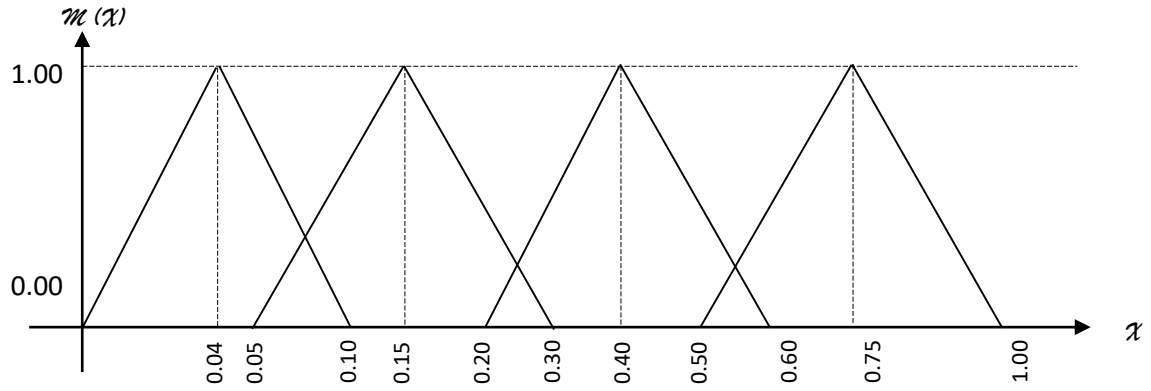
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



18- dst_host_srv_diff_host_rate

Scale: 0.00 – 1.00

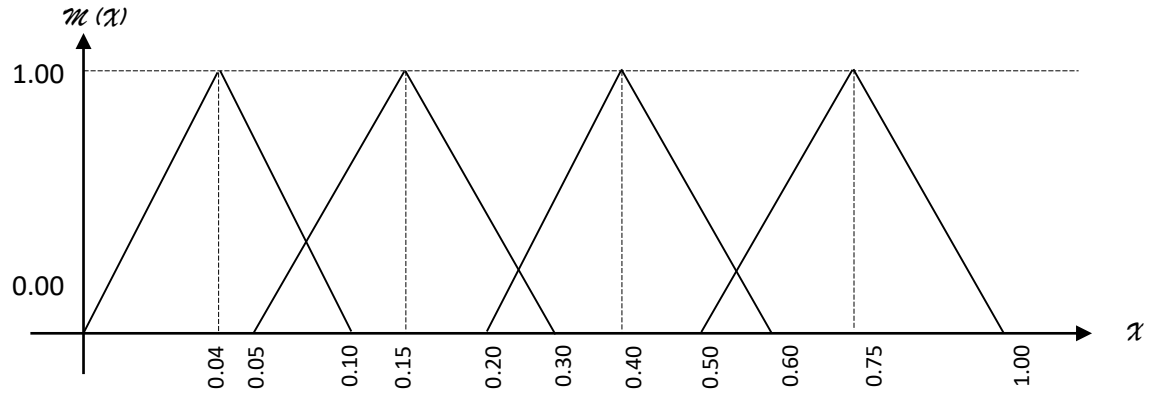
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



19- dst_host_serror_rate

Scale: 0.00 – 1.00

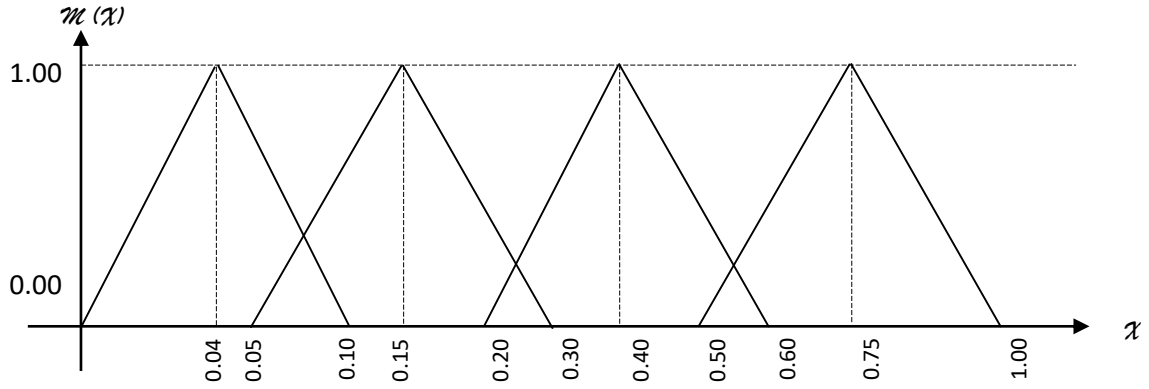
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



20- dst_host_srv_serror_rate

Scale: 0.00 – 1.00

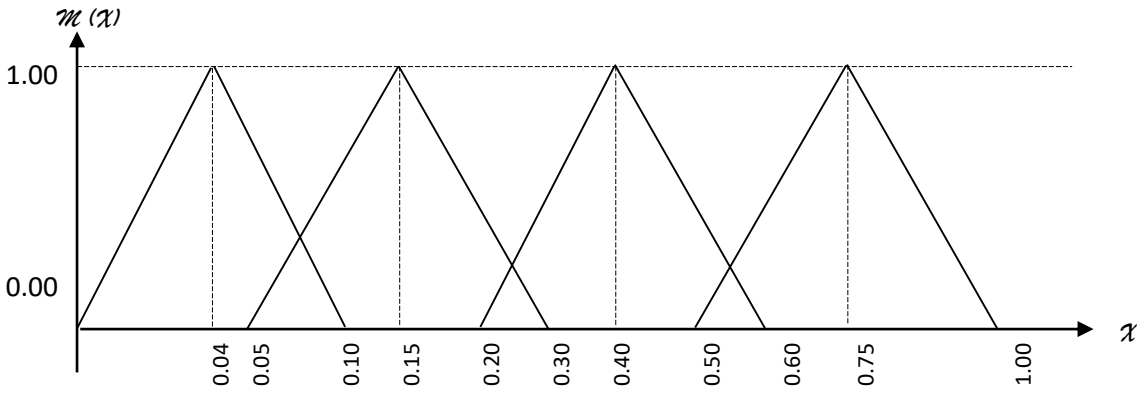
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



21- dst_host_rerror_rate

Scale: 0.00 – 1.00

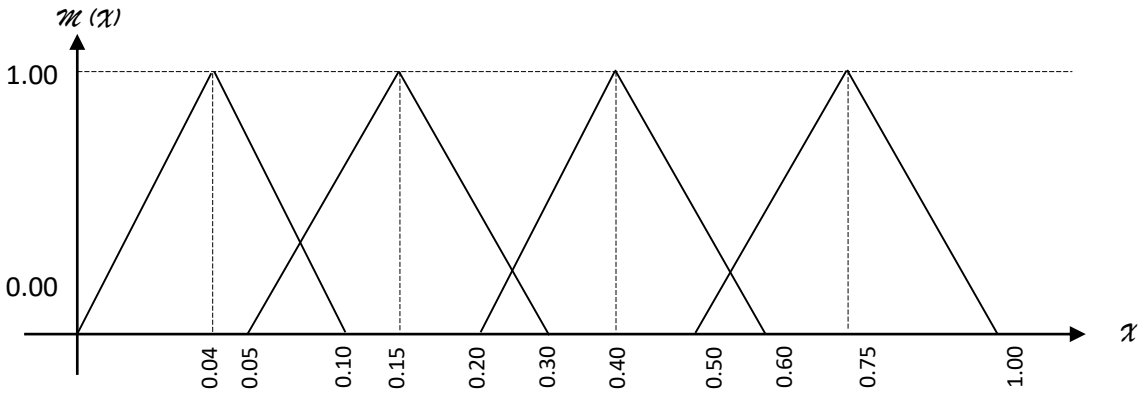
FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



22- dst_host_srv_error_rate

Scale: 0.00 – 1.00

FSs: vfew<0.00,0.04,0.10>; few<0.05,0.15,0.30>; average<0.20,0.40,0.60>; many<0.50,0.75,1.00>



Appendix C: Rule Knowledge Base (Samples)

	1	2	3	4	5	6	7	8	60
Rule #	Duration	protocol_type	service	flag	src_bytes	dest_bytes	Land	wrong_fragment	Attack Name
R001	xlong	TCP	http		xxmany				Apache2
R002	vshort	ICMP	echo_i	SF	xmany				Smurf
R003		TCP		S0					Neptune
R004			netbios						DoSNuke
R005		TCP					1		Land
R006	average	ICMP			xmany			> 0	POD
R007	short	TCP	http		xxmany	xmany			Back
R008	average	UDP	private					>= 3	Teardrop
R009		TCP		RTSO					TcpReset
R010		UDP							Syslogd
R011	short	TCP	http	S1					CrashIIS
R012	short	ICMP	dhcp	ecr_i					ARPPoison
R013	short	TCP	SMTP		xxmany	few			MailBomb
R014		ICMP		Echo_Request	vfew				Selfping
R015	xxlong	TCP	port 79						Processtable
R016		UDP	echo - private					>= 2	UDPstorm
R017		TCP	http						http GET flooding
R018			ssh						SSHprocesstable
R019		TCP - ICMP	eco_i						IPSweep
R020	long	TCP		SH - SHR					Queso
R021				REJ					Saint
R022		UDP		REJ					Satan
R023	short	TCP							MScan

	1	2	3	4	5	10	11	12	60
Rule #	Duration	protocol_type	service	flag	src_bytes	Hot	num_failed_logins	logged_in	Attack Name
R028	long	TCP - ICMP	chargen - port143						Portsweep
R029	long								Nmap
R030			telnet - ftp - pop - imap				>= 3	> 0	Dictionary
R031			DNS			> 1		> 1	Netcat
R032			SMTP		xxmany		>=2		SendMail
R033	average	TCP	imap			> 1			Imap
R034			ftp			> 2		1	NcFTP
R035	average	TCP			xxmany			1	Xlock
R036	short	TCP			xxmany				Xsnoop
R037			SSH				>=2		SSHTrojan
R038			smtp						FrameSpoofer
R039	short		telnet - rlogin				>2		Guest
R040		TCP		S1				1	Netbus
R041		TCP	ftp - ftp_data - priter		many				FTPWrite
R042	long	TCP						1	HttpTunnel
R043		TCP	http			> 1		1	Phf
R044	long	TCP	Telnet	SF	many				Spy
R045		UDP	private	SF	few				SNMP GET Attack
R046	short	UDP	private				> 1	1	SNMP Guess Attack
R047	short	TCP	DNS		many - xxmany				Named
R048	average	TCP	FTP - Telnet - POP3 - IMAP - SSH		few		> 0		Guess Password
R049	long	TCP			many	> 2			Multihop
R050	long	TCP	FTP_Data		xmany				WarezMaster
R051		TCP			many				Ppmacro
R052	short	TCP	FTP - FTP_Data		many				WarezClient