AN EFFICIENT ANOMALY INTRUSION DETECTION METHOD WITH EVOLUTIONARY NEURAL NETWORK

SAMIRA SARVARI

FSKTM 2020 17

AN EFFICIENT ANOMALY INTRUSION DETECTION METHOD WITH EVOLUTIONARY NEURAL NETWORK

By

SAMIRA SARVARI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

February 2020

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

AN EFFICIENT ANOMALY INTRUSION DETECTION METHOD WITH EVOLUTIONARY NEURAL NETWORK

By

SAMIRA SARVARI

February 2020

Chairman : Associate Professor Nor Fazlida Mohd Sani, PhD
Faculty : Computer Science and Information Technology

Anomaly-based intrusion detection plays a vital role in protecting networks against malicious activities. Despite all the strengths of the anomaly detection systems, there are still drawbacks that reduce the performance of the system. One of the technical challenges is to examine a large amount of data which makes a large number of computations and low detection rates problematic. Another critical issue in anomaly detection is to produce a high false alarm rate that reduce the efficiency of the system. In recent years, detection methods based on machine learning techniques are widely deployed in order to improve the efficiency of anomaly-based detection. Among these techniques, Artificial Neural Network-Multilayer Perceptron (ANN-MLP) is one of the significant used techniques that has been successful in solving many complex practical problems. However, ANN-MLP without activation function would simply be a linear regression model which has limitation and does not perform well most of the times. Although activation functions are important for MLP to learn but for non-linear complex functional mappings it has complicated calculation which reduces the accuracy of classification.

To overcome the aforementioned issues, in this research proposed anomaly based detection is designed with Evolutionary Neural Network (ENN) by three different detection methods. The first anomaly detection method is designed using a new feature selection technique called Mutation Cuckoo Fuzzy (MCF) and evolutionary neural network classification called MultiVerse Optimizer- Artificial Neural Network (MVO-ANN) to improve the performance and execution time. The second anomaly detection method is the Evolutionary Kernel Neural Network Random Weights (EKNNRW) in order to increase the accuracy of classification. The third proposed method is a new Evolutionary Neural Network (ENN) algorithm with a combination of Genetic Algorithm and Multiverse Optimizer (GAMVO) as a training part of ANN to create efficient anomaly-based detection with low false alarm rate. The proposed

methods have been applied to the problem of intrusion detection and validated based on the famous dataset NSL-KDD.

Based on the first method, the result of execution time for the proposed method (MCF & MVO-ANN) is 60.33s, while previous research (MVO-ANN) indicates 163.07s in second. Furthermore, performance of proposed method is much improved as compared to previous research. In the second method (EKNNRW), accuracy obtained 99.24% whereas accuracy in previous research was 98.03%. The experiment results show that not only accuracy also detection rate and false alarm rate have had an exhibitive improve. The third proposed method (GAMVO-ANN) obtained detection rate and false alarm rate of 98.65% and 0.012% respectively which outperforming the previous research and the two previous methods proposed in this research. Several directions can be taken to extend this work such as a combination of an IDS with the IPS system to be capable of dropping or blocking network connections that are determined too risky, extend the model for multi-class classification problems and using hybrid IDS (combining anomaly and signature-based detection systems) to respond to wider ranges of intrusions and increase the level of security of a network.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

KAEDAH PENGESANAN PENCEROBOHAN ANOMALI BERKESAN DENGAN RANGKAIAN NEURAL EVOLUSIONARI

Oleh

SAMIRA SARVARI

Februari 2020

Pengerusi : Profesor Madya Nor Fazlida Mohd Sani, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Pengesanan pencerobohan berasaskan anomali memainkan peranan penting dalam melindungi rangkaian terhadap aktiviti hasad. Walaupun semua kekuatan sistem pengesanan anomali, masih terdapat kekurangan yang melemahkan prestasi sistem tersebut. Salah satu cabaran teknikal adalah untuk meneliti sejumlah besar data yang menyebabkan sebilangan besar perkomputeran dan kadar pengesanan yang rendah bermasalah. Isu kritikal lain dalam pengesanan anomali adalah untuk menghasilkan kadar isyarat palsu yang tinggi yang mengurangkan kecekapan sistem tersebut. Sejak akhir ini, kaedah pengesanan berasaskan teknik pembelajaran mesin telah digunakan secara meluas bagi mempertingkatkan kecekapan pengesanan berasaskan anomali. Antara teknik tersebut, Perseptron Rangkaian Neural Artifisial Multilapisan (ANN-MLP) merupakan salah satu teknik terpakai yang signifikan yang telah berjaya dalam menyelesaikan banyak masalah praktikal yang kompleks. Walau bagaimanapun, ANN-MLP tanpa fungsi pengaktifan hanya merupakan model regresi linear yang mempunyai limitasi dan tidak dilaksanakan dengan baik bagi kebanyakan masa. Walaupun fungsi pengaktifan adalah penting bagi MLP untuk dipelajari tetapi bagi pemetaan fungsional kompleks bukan linear, ia mempunyai pengiraan yang rumit yang mengurangkan ketepatan pengklasifikasian.

Bagi mengatasi isu tersebut, dalam penyelidikan ini pengesanan berasaskan anomali yang dicadangkan telah direka bentuk dengan Rangkaian Neural Evolusionari (ENN) melalui tiga kaedah pengesanan yang berbeza. Kaedah pengesanan anomali pertama telah direka bentuk menggunakan teknik pemilihan fitur baharu yang dinamakan Mutasi Cuckoo Kabur (MCF) dan pengklasifikasian rangkaian neural evolusionari yang dinamakan MultiVerse Optimizer-Artificial Neural Network (MVO-ANN) bagi meningkatkan prestasi dan masa perlaksanaan. Kaedah pengesanan anomali kedua ialah Pemberat Rawak Neural Kernel Evolusionar (EKNNRW) bagi meningkatkan ketepatan pengkalsifikasian. Kaedah dicadangkan yang ketiga ialah algoritma

Rangkaian Neural Evolusionari (ENN) yang baharu beserta kombinasi Algoritma Genetik dan Pengoptimum Multirangkap (GAMVO) sebagai sebahagian latihan ANN bagi menghasilkan pengesanan berasaskan anomali yang efisien dengan kadar isyarat palsu yang rendah. Kaedah yang dicadangkan telah diaplikasikan pada masalah pengesanan pencerobohan dan telah divalidasi berdasarkan dataset NSL-KDD yang terkenal.

Berdasarkan kaedah pertama, dapatan masa perlaksanaan bagi kaedah yang dicadangkan (MCF& MVO-ANN) ialah 60.33s, manakala penyelidikan terdahulu (MVO-ANN) memperlihatkan 163.07s dalam saat. Di samping itu, prestasi kaedah yang dicadangkan adalah begitu meningkat berbanding dengan penyelidikan terdahulu. Dalam kaedah kedua (EKNNRW), ketepatan diperoleh ialah 99.24% manakala ketepatan dalam penyelidikan terdahulu ialah 98.03%. Dapatan eksperimen menunjukkan bahawa bukan hanya ketepatan, tetapi juga kadar pengesanan dan kadar isyarat palsu telah memperlihatkan peningkatan yang memberangsangkan. Kaedah ketiga yang dicadangkan (GAMVO-ANN) memperoleh kadar pengesanan dan kadar isyarat palsu, masing-masing 98.65% dan 0.012% yang mendahului penyelidikan terdahulu dan dua kaedah terdahulu yang dicadangkan dalam penyelidikan ini. Beberapa arah tuju dapat diambil bagi memperluas kajian ini seperti kombinasi IDS dengan sistem IPS yang berupaya menggugur atau menyekat sambungan rangkaian yang didapati terlalu berisiko, memperluas model bagi masalah pengklasifikasian multikelas dan menggunakan IDS hibrid (kombinasi anomali dan sistem pengesanan berasaskan signatur) bagi memberi respon kepada pelbagai bentuk pencerobohan yang lebih luas dan oleh itu dapat meningkatkan tahap keselamatan sesebuah rangkaian.

ACKNOWLEDGEMENTS

"GOD Thank you for giving me the strength and encouragement especially during all the challenging moments in completing this thesis. I am truly grateful for your exceptional love and grace during this entire journey".

I would like to express my sincere appreciation and deepest gratitude to my supervisor Associate Prof. Dr. Nor Fazlida Mohd Sani and my committee members Associate Prof. Dr. Zurina Mohd Hanapi and Associate Prof. Dr. Mohd Taufik Abdullah for their continuous encouragement, valuable advice, and guidance throughout this research. They are the backbone of this project by giving wonderful suggestions and constructive criticism which gave this study a life.

I would like to express my unfailing gratitude and love to my husband, who has supported me throughout this process and has constantly encouraged me when the tasks seemed arduous and insurmountable.

I also owe much gratitude to my beloved parents, my parents-in-law and my siblings for their unwavering support and prayers.

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Nor Fazlida Mohd Sani, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zurina Mohd Hanapi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Mohd Taufik Abdullah, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 11 June 2020

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: ________________________________ Date:________________

Name and Matric No: Samira Sarvari, GS42239

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: ________________________
Name of Chairman of Supervisory Committee: Associate Professor Dr. Nor Fazlida Mohd Sani

Signature: ________________________
Name of Member of Supervisory Committee: Associate Professor Dr. Zurina Mohd Hanapi

Signature: ________________________
Name of Member of Supervisory Committee: Associate Professor Dr. Mohd Taufik Abdullah

TABLE OF CONTENTS

				Page
ABSTRACT				i
ABSTRAK				iii
ACKNOWLEDGEMENTS				v
APPROVAL				vi
DECLARATION				viii
LIST OF TABLES				xiii
LIST OF FIGURES				xiv
LIST OF ABBREVIATIONS				xvii
CHAPTER				
1	**INTRODUCTION**			1
	1.1	Background		1
	1.2	Motivation		2
	1.3	Problem Statement		4
	1.4	Research Objectives		5
	1.5	Scope of Research		5
	1.6	Research Contributions		6
	1.7	Thesis Organization		6
2	**LITERATURE REVIEW**			8
	2.1	Security		8
	2.2	Intrusion Detection System (IDS)		8
	2.3	Characteristics of IDS		9
	2.4	IDS Types		10
	2.5	IDS Techniques		11
	2.6	Types of machine learning techniques		13
	2.7	IDS Feature Selection		14
	2.8	The General Feature Selection Approaches		15
		2.8.1	Wrapper Method	16
		2.8.2	Filter Method	16
		2.8.3	Hybrid Method	17
	2.9	Optimization Algorithm		20
		2.9.1	Swarm-based algorithms	20
			2.9.1.1 Cuckoo Search Algorithm (CSA)	21
		2.9.2	Evolutionary Algorithm (EA)	23
			2.9.2.1 Multiverse Optimizer (MVO)	24
		2.9.3	Trajectory-based algorithms	26
	2.10	Classification of ML techniques		26
		2.10.1	Clustering	27
		2.10.2	Fuzzy Logic (FL)	27
		2.10.3	Decision Trees (DT)	27
		2.10.4	K-Nearest Neighbour (K-NN)	28
		2.10.5	Support Vector Machine (SVM)	28
		2.10.6	Genetic Algorithm (GA)	29

		2.10.7 Bayesian Network (BN)	29
		2.10.8 Artificial Neural Network (ANN)	29
	2.11	A Decade of IDS using ML techniques	30
	2.12	Artificial Neural Network in IDS	36
		2.12.1 Kernel Neural Network in IDS	39
		2.12.2 Evolutionary Neural Network in IDS	39
	2.13	Summary	43
3	**RESEARCH METHODOLOGY**		**44**
	3.1	Introduction	44
	3.2	Research Methodology	44
	3.3	Problem Formulation	46
	3.4	Data Preparation	46
	3.5	Implementation and Analysis of Previous IDS Model (MVO-ANN)	50
		3.5.1 Experimental Setup and Results (MVO-ANN)	51
		3.5.2 Experimental Setup and Results (Benchmark)	52
	3.6	Proposed New IDS Models	55
		3.6.1 Method (1): (MCF&MVO-ANN)	56
		3.6.2 Method (2): (EKNNRW)	56
		3.6.3 Method (3): (GAMVO-ANN)	56
	3.7	Performance Metrics Evaluation	56
	3.8	Summary	58
4	**A NEW FEATURE SELECTION METHOD TO IMPROVE EXECUTION TIME AND PERFORMANCE OF IDS**		**59**
	4.1	Introduction	59
	4.2	The proposed anomaly-based detection method (MCF & MVO-ANN)	59
		4.2.1 Cuckoo Search Algorithm (CSA)	61
		4.2.2 Cuckoo Search with Fuzzy C Means	63
		4.2.3 Mutation Cuckoo Search Algorithm	64
		4.2.4 Multiverse Optimization (MVO)	68
		Training of ANN with the MVO algorithm	70
	4.3	Experimental results	71
	4.4	Summary	79
5	**EVOLUTIONARY KERNEL NEURAL NETWORK RANDOM WEIGHTS TO IMPROVE ACCURACY OF CLASSIFICATION**		**80**
	5.1	Introduction	80
	5.2	The proposed anomaly-based detection method (EKNNRW)	80
		Training of KNNRW with the MVO algorithm	86
	5.3	Experimental results	89
	5.4	Summary	94

6	**COMBINATION OF MODIFIED EVOLUTIONARY ALGORITHM AND ARTIFICIAL NEURAL NETWORK TO REDUCE FALSE ALARM RATE**		95
	6.1	Introduction	95
	6.2	The proposed anomaly-based detection method (GAMVO-ANN)	95
	6.3	Experimental results	107
	6.4	Summary	112
7	**CONCLUSION**		113
	7.1	Summary	113
	7.2	Future works	115
REFERENCES			116
BIODATA OF STUDENT			128
LIST OF PUBLICATIONS			129

LIST OF TABLES

Table		Page
2.1	Some techniques of feature selection in IDS	18
2.2	Summary of recent modifications to CSA	22
2.3	Hard and soft clustering	27
2.4	A Decade of IDS using ML techniques (2008 - 2018)	33
2.5	Artificial Neural Network techniques-based IDS	38
2.6	Evolutionary Neural Network based IDS	41
3.1	Description and overall picture of the NSL-KDD dataset	47
3.2	Mapping of attack class with attack type	48
3.3	Transformation table	49
3.4	Statistics of the NSL-KDD dataset	50
3.5	Performance test result of MVO-ANN	52
3.6	Results obtained from 30 times running	54
3.7	Average results obtained from 30 times running	54
3.8	Possibilities to classify events	57
4.1	Selected features using proposed feature selection (MCF)	67
4.2	NSL-KDD features used by each methods	72
4.3	Results obtained from 30 times running proposed method (MCF&MVO-ANN)	76
4.4	Performance average results of MCF&MVO-ANN	77
5.1	Results obtained from 30 times running of EKNNRW	92
5.2	Performance average results of EKNNRW	92
6.1	Results obtained from 30 times running of GAMVO-ANN	110
6.2	Performance average results of GAMVO-ANN	110

LIST OF FIGURES

Figure		Page
1.1	General Incident Classification (MyCERT)	3
2.1	An architecture of IDS	9
2.2	IDS classifications	10
2.3	Classification of anomaly-based detection systems	11
2.4	Classification of statistical based	12
2.5	Classification of knowledge based	12
2.6	Feature selection process	15
2.7	Wrapper method process	16
2.8	Filter method process	16
2.9	Hybrid method process	17
2.10	Classification of Optimization Algorithms	20
2.11	Instances of swarm-based algorithms	21
2.12	Instances of Evolutionary Algorithms	23
2.13	Instances of Trajectory-based algorithms	26
2.14	Classification of Machine Learning	26
3.1	Research Methodology	45
3.2	IDS model proposed	50
3.3	Detection rate performance results comparison	52
3.4	Accuracy performance results comparison	53
3.5	False alarm rate performance results comparison	53
3.6	Proposed IDS Models	55
4.1	The proposed IDS model (MCF&MVO-ANN)	60
4.2	Cuckoo Search Algorithm	62
4.3	The process of using FCM in CS	64

4.4	The general steps of the proposed feature selection (MCF)	66
4.5	Simple architecture of the ANN	68
4.6	General training of the MVO-ANN	71
4.7	Execution time results comparison	72
4.8	The priority of selected features	73
4.9	Accuracy of results for each priority	74
4.10	Accuracy performance results comparison	74
4.11	Detection rate performance results comparison	75
4.12	False alarm rate performance results comparison	75
4.13	Accuracy performance average results comparison	77
4.14	Detection rate performance average results comparison	78
4.15	False alarm rate performance average results comparison	78
5.1	The proposed IDS model (EKNNRW)	81
5.2	The fundamental unit of an ANN-MLP	82
5.3	The flowchart of proposed algorithm (KNNRW)	86
5.4	The general training of the MVO-KNNRW	88
5.5	Accuracy performance results comparison	89
5.6	Accuracy performance results comparison with other models	90
5.7	Detection rate performance results comparison	91
5.8	False alarm rate performance results comparison	91
5.9	Accuracy performance average results comparison	93
5.10	Detection rate performance average results comparison	93
5.11	False alarm rate performance average results comparison	94
6.1	The proposed IDS model (GAMVO-ANN)	96
6.2	Simple architecture of the ANN	97
6.3	The standard steps of the MVO Algorithm	101

6.4	The generic genetic algorithm	103
6.5	Combination of GA and MVO	105
6.6	General training of the GAMVO-ANN	106
6.7	False alarm rate performance results comparison	107
6.8	False alarm rate performance results comparison with other models	108
6.9	Detection rate performance results comparison	109
6.10	Accuracy performance results comparison	109
6.11	Accuracy performance average results comparison	111
6.12	Detection rate performance average results comparison	111
6.13	False Alarm rate performance average results comparison	112

LIST OF ABBREVIATIONS

ABC	Artificial Bee Colony
ACC	Accuracy
ADS	Anomaly-based Detection System
AI	Artificial Intelligence
ANN	Artificial Neural Network
BP	Back Propagation
BN	Bayesian Network
CSA	Cuckoo Search Algorithm
DCSA	Discrete CSA
DM	Data Mining
DR	Detection Rate
DT	Decision Tree
EA	Evolutionary Algorithm
EKNNRW	Evolutionary Kernel Neural Network Random Weights
ENN	Evolutionary Neural Network
ET	Execution Time
FA	Firefly Algorithm
FAR	False Alarm Rate
FN	False Negative
FNN	Feed-Forward Neural Network
FP	False Positive
FS	Feature Selection
GA	Genetic Algorithm

GAMVO	Genetic Algorithm-Multiverse Optimizer
GCS	Gauss Cuckoo Search
HIDS	Host-based IDS
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
K-NN	K-Nearest Neighbour
LNS	Local Network System
MCF	Mutation Cuckoo Fuzzy
MCSA	Multi-Objective Cuckoo Search Algorithm
ML	Machine Learning
MLP	Multilayer Perceptron
MSE	Mean Squared Error
MVO	Multiverse Optimizer
MyCERT	Malaysia Computer Emergency Response Team
NIDS	Network-based IDS
PSO	Particle Swarm Optimization
RBF	Radial Basis Function
SI	Swarm Intelligence
SSO	Site Security Officer
SVM	Support Vector Machine
TDR	Travelling Distance Rate
TN	True Negative
TP	True Positive
WEP	Wormhole Existence Probability

CHAPTER 1

INTRODUCTION

This chapter discusses the background of the study, the motivation of the research, research problems, objectives, scope and contributions of research.The chapter ends with an outline of the organization of the thesis.

1.1 Background

In today's world, with the tremendous growth of network-based services and sensitive information on networks, network security is getting more important than ever (Swisscom, 2019) Intrusion Detection System (IDS) become an inseparable part of each computer networks due to, it capable to detect threats that originate from both inside and outside a network before they damage organizations' valuable information. Therefore, the focus of this research is to enhance network security using IDS.

In recent years, IDS has become one of the significant research areas in computer security. It is an important detection technology and is used as a countermeasure to preserve data integrity and system availability during an intrusion (Hajamydeen & Udzir, 2019). The basic task in IDS is to learn "what is normal" and "what is abnormal or an attack" and represent this knowledge to further alleviate security related problems. From this point of view, techniques from various disciplines have been applied to build efficient systems. Based on the detection technique, there are two (2) types of IDS. There are misuse-based, also known as signature-based that can detect known attacks and anomaly-based that able to detect unknown attacks as well (Axelsson, 2000).

Since the existing intrusion detection algorithms still have some shortcomings and unable to detect the complex nature of the new attacks in networks this research mainly targets the anomaly-based intrusion detection system. Many approaches have been applied to anomaly-based detection. Data mining is the first proposed system for building an IDS which doing the process of extracting knowledge and useful information from an extensive database (Fu & Lui, 2007) .It helps to extract rule patterns from a knowledge base and use them to predict future intrusion in similar datasets. However, most of them have limitations. They are unable to detect new attacks with new signatures since they don't have these signatures in their knowledge base. All new unknown attacks go unnoticed until the system has updated its knowledge base. Though, the constant update of the rules in a knowledge base makes it difficult to manage and maintain these approaches and have difficulty to detect the complex nature of the new attacks in networks (Benmessahel, Xie, & Chellal, 2017). Machine learning approaches have been proposed in recent years to overcome these limitations (Sarvari, Muda, Ahmad, & Barati, 2015).

One of the most widely used machine learning techniques is Artificial Neural Networks (ANN). Combination of ANN and Evolutionary Algorithm (EA) can produce an advanced technique to develop an efficient anomaly detection approach for IDS (Benmessahel, Xie, Chellal, & Semong, 2019). Evolutionary Neural Network (ENN) algorithm is a form of neural network in which evolution is fundamental in the optimization of its learning process (Yao, 1993). In this study, three stepwise methods using ENN proposed in order to improve the efficiency of anomaly-based detection.

1.2 Motivation

As the number of data networks, digital applications, as well as internet and mobile users is growing, so do the chances of cyber exploitation and cybercrimes. Even a small mistake in securing data or bad social networking can prove to be extremely dangerous. Last few decades, there is an urgent need to secure the operations in computer systems and networks for both private and governmental institutions which are relying heavily on networking and the internet. The security perspective is part of the protection and evaluation process for the computer system and its network resources such as stability, flexibility, reliability, confidentiality, availability, and integrity for most aspects of critical information data.

Data from the Malaysia Computer Emergency Response Team (MyCERT)[1] depicted a significant growth in cyber-attacks as shown in Figure 1.1. Cyber-attacks have become a novel weapon of war around the world and their persistent growth against computer and network systems makes it critical to integrate more accurate IDS capable of maximizing correctly detectable data (i.e., true positives and negatives) and minimizing falsely detectable data (false positives and negatives) to enable prompt identification of attacks.Recently researchers have got a promised interest in the intrusion detection area by designing various approaches to get good results in this field. The necessity for continuous enhancement of intrusion detection capabilities, in terms of the execution time, accuracy, detection rate and false alarm rates are the motivation for this research.

[1] https://www.mycert.org.my/

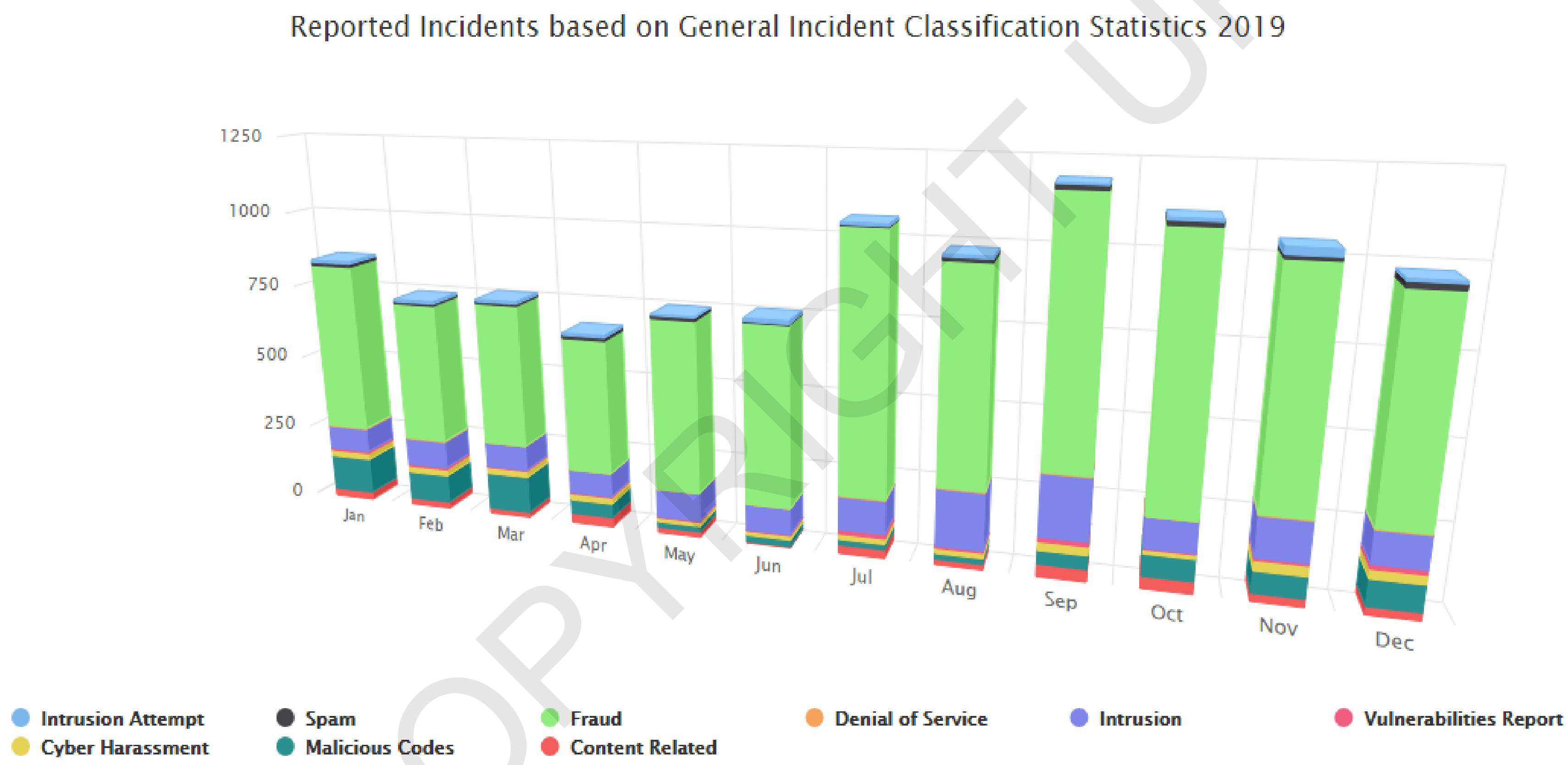

Figure 1.1 : General Incident Classification (MyCERT)

1.3 Problem Statement

Based on literature studies, a few problems have been discovered in this research. This research explains the problems starting from the massive data, followed by the accuracy of classification in ANN-MLP and then high false alarm rate in anomaly-based detection.

A large amount of data that contain irrelevant and redundant features is a technical challenge in intrusion detection systems.In the last three decades, computer networks have grown in size and complexity drastically. This tremendous growth has posed challenging issues in network and information security (Mohammadi, Mirvaziri, Ghazizadeh-Ahsaee, & Karimipour, 2019). According to the characteristics of IDS, time performance is one of the important factors. Execution time is the amount of time that passes from the start of an event to its finish. Considering that new attacks are growing quickly, they have to be detected before any damage is caused to the system or data. Based on machine learning techniques for detecting attacks, data is divided into two categories: a training set and testing set which part of the time is devoted to learning . Massive data may increase overfitting because some features are irrelevant or redundant and there is more opportunity to complicate the model and increase the training time that leads to high execution time (Chiba, Abghour, Moussaid, El omri, & Rida, 2019).

Among many techniques available for anomaly detection system, classification algorithms have been demonstrated to produce impressive and efficient results in detecting attacks (Aziz, Hanaf, & Hassanien, 2017). Another problem is the accuracy of classification using Artificial Neural Network-Multilayer Perceptron (ANN-MLP) is not efficient enough. Due to complicated calculations to transfer data that sometimes subjected to errors . The most important property of an ANN-MLP is its generalization ability in solving complex problems but without activation function would simply be a linear regression model, which has limitations and does not perform well most of the time (Cahyo, Hidayat, & Adhipta, 2016). It needs an activation function to deal with nonlinear phenomena. However, this approach not only has complicated calculations it is only useful if the available parametric function catalog fits the data nicely otherwise, it faces the problem of data differentiation and will reduce the accuracy of classification (Hussain, Lalmuanawma, & Chhakchhuak, 2016).

Anomaly-based detection works by training itself to recognize acceptable behavior and then raising an alarm for any behavior outside the boundaries of its training. The training part has a significant role to detect the complex nature of the new attacks (Viegas, Santin, & Oliveira, 2017). The third problem is a high false-positive rate in anomaly-based detection. However, the ANN-MLP is one of the most widely used techniques and has successfully solved many complex practical problems that are difficult to solve through other methods, but it has limitation in training process using the well-known training algorithm Back-Propagation (BP). BPANN system presents many parameters (i.e., weight, activation function and gradient information) within the ANN structure. Also, it gets into local structural minima, which negatively affects the capability of accurately assigning the ANN structures which negatively affects the capability of ANN-MLP based IDS (Benmessahel, Xie, & Chellal, 2017).

Based on the mentioned constraints, this study addresses the following issues:

1. The huge amount of data that contain irrelevant and redundant features increase the execution time in anomaly-based detection.
2. Accuracy of classification based on ANN-MLP is not efficient enough due to complicated calculation for mapping data from the original space to higher dimensional feature space.
3. Anomaly-based detection has difficulty to detect the complex nature of the new attacks in networks and failure to distinguish the behaviour cause generates a huge amount of false-positive alarms.

1.4 Research Objectives

The main objective of this research is to propose an efficient anomaly detection method with an evolutionary neural network which is able to maintain high efficiency and detect attacks more accurately. In order to achieve this goal, three different kinds of detection methods have been proposed in this research.

1. To propose an anomaly-based detection using a new suggested feature selection and evolutionary neural network classification to reduce the number of features by removing irrelevant and redundant features in order to improve the execution time and performance of anomaly detection system.
2. To propose an anomaly-based detection using an evolutionary neural network with a combination of kernel and random weights method which able to increase the accuracy of classification to detect attacks and normal.
3. To propose an evolutionary neural network with the new proposed evolutionary algorithm as a training part of the artificial neural network to create an efficient anomaly-based detection with low false alarm rate.

1.5 Scope of Research

This research focuses on an anomaly-based detection method which utilizes an evolutionary neural network by three different new proposed methods to accurately identify intrusive and non-intrusive behaviour. In addition, proposed detection methods are designed such that they could improve the performance of IDS in terms of accuracy, detection rate and false alarm rate. The scope is also on reducing execution time by removing irrelevant and redundant features.The dataset used in this research is the well-known NSL-KDD dataset which is one of the best candidate datasets for simulating and testing the performance of IDS to assess the proposed, individual, and existing detection methods.

1.6 Research Contributions

The major contribution of this research is the creation of an anomaly detection method that could identify an intrusive and non-intrusive behaviours more accurately and to improve the efficiency of anomaly based detection system.

1. Developing an anomaly-based detection using a new proposed feature selection method called Mutation Cuckoo Fuzzy (MCF) and Evolutionary Neural Network (MVO-ANN) classification to improve the execution time and performance of IDS by removing the irrelevant and redundant features. Experiments show that the proposed model is capable of detecting attacks more rapidly with high efficiency.
2. Creating an anomaly-based detection using an Evolutionary Kernel Neural Network Random Weights (EKNNRW) to differentiate and identify the behaviours of an attack and normal more accurately, particularly which able to increase the accuracy of classification. This method has shown remarkable outcomes and improvements for all aforesaid factors which directly improved the accuracy of classification as compared to the previous research.
3. Designing an evolutionary neural network with the new proposed evolutionary algorithm using the combination of the Genetic Algorithm and Multiverse Optimizer (GAMVO) as a training part of ANN-MLP to create an efficient anomaly-based detection with low false alarm rate. In comparison with the individual and existing methods, this approach has achieved impressive results and improved the detection and false alarm rates.

1.7 Thesis Organization

This section presents an outline of the entire thesis which is organized as follows:

Chapter 1 presents the background, motivation, problem statement, research objectives as well as scope of the thesis.

Chapter 2 reviews related studies of the subject matter which includes intrusion detection systems (IDSs), it's types and techniques with focusing on anomaly-based detection. This chapter also provides a summary of machine learning and importance of them for improving IDS.

Chapter 3 provides detailed discussions of the research methodologies adopted in this research. The research methodology gives step-by-step guidance to the reader to understand this research. Also, requirement analysis involved in the process of identification and investigation of the research requirement is detailed out.

Chapter 4 describes the design and evaluation of the proposed anomaly detection method using Mutation Cuckoo Fuzzy (MCF) feature selection and evolutionary neural network classification.

Chapter 5 describes the design and evaluation of the proposed anomaly detection method using evolutionary kernel neural network random weights.

Chapter 6 describes the design and evaluation of the proposed anomaly detection method using combination of Genetic and Multiverse Optimizer (GAMVO) algorithm as evolutionary algorithm and Artificial Neural Network.

Chapter 7 conclude the work and recommended some promising direction for future research.

REFERENCES

Acharya, N., & Singh, S. (2017). An IWD-based feature selection method for intrusion detection system. *Soft Computing*, *22*(13), 4407–4416. https://doi.org/10.1007/s00500-017-2635-2

Afifi, A., Zanaty, E. A., & Ghoniemy, S. (2013). Improving the Classification Accuracy Using Support Vector Machines (Svms) With New Kernel. *Journal of Global Research in Computer Science*, *4*(2), 1–7.

Aghdam, M. H., & Kabiri, P. (2016). Feature selection for intrusion detection system using ant colony optimization. *International Journal of Network Security*, *18*(3), 420–432.

Ahmad, I., Abdullah, A., Alghamdi, A., Alnfajan, K., & Hussain, M. (2011). Intrusion detection using feature subset selection based on MLP. *Scientific Research and Essays*, *6*(34), 6804–6810. https://doi.org/10.5897/SRE11.142

Ahmed, I. M. (2016). Enhancement of Network Attack Classification using Particle Swarm Optimization and Multi Layer-Perceptron. *International Journal of Computer …*, *137*(12), 18–22.

Akhlaghi, R., & Lotfi, R. (2020). Robust Optimization of Routing Robot for Prediction , Estimation and Target Trajectory based on Bat Algorithm Robust Optimization of Routing Robot for Prediction , Estimation and Target Trajectory based on Bat Algorithm. *International Journal of Industrial Engineering and Operational Research (IJIEOR)*, (January).

Alamiedy, T. A., Anbar, M., & Al-ani, A. K. (2019). Review on Feature Selection Algorithms for Anomaly-Based Intrusion Detection System. *Springer Nature Switzerland*, (January). https://doi.org/10.1007/978-3-319-99007-1

Alomari, O., & Othman, Z. A. (2012). Bees algorithm for feature selection in network anomaly detection. *Journal of Applied Sciences Research*, *8*(3), 1748–1756.

Amruthnath, N., & Gupta, T. (2018). A Research Study on Unsupervised Machine Learning Algorithms for Early Fault Detection in Predictive Maintenance. *Computers and Electrical Engineering*, (August 1993), 355–361. https://doi.org/10.13140/RG.2.2.28822.24648

Aslahi-Shahri, B. M., Rahmani, R., Chizari, M., Maralani, A., Eslami, M., Golkar, M. J., & Ebrahimi, A. (2015). A hybrid method consisting of GA and SVM for intrusion detection system. *Neural Computing and Applications*, *27*(6), 1669–1676. https://doi.org/10.1007/s00521-015-1964-2

Assi, J. H., & Sadiq, A. T. (2017). NSL-KDD dataset Classification Using Five Classification Methods and Three Feature Selection Strategies. *Journal of Advanced Computer Science and Technology Research*, *7*(1), 15–28.

Axelsson, S. (2000). Intrusion Detection Systems: A Survey and Taxonomy. *International Journal of Innovative Technology and Exploring Engineering*, *99*, 1–15. https://doi.org/10.1.1.1.6603

Axelsson, & Sands. (2016). Undrestanding Intrusion Detection System Through Visualization. *Springer International Publishing*. Retrieved from https://link.springer.com/article/10.1007/s10489-017-1085-z

Azeez, N. A., Bada, T. M., Misra, S., Adewumi, A., Van der Vyver, C., & Ahuja, R. (2020). Intrusion Detection and Prevention Systems: An Updated Review. *Advances in Intelligent Systems and Computing*, *1042*(October 2019), 685–696. https://doi.org/10.1007/978-981-32-9949-8_48

Aziz, A. S. A., Hanaf, S. E.-O., & Hassanien, A. E. (2017). Comparison of classification techniques applied for network intrusion detection and classification. *Journal of Applied Logic*, *24*, 109–118. https://doi.org/10.1016/j.jal.2016.11.018

Aziz, M. A. El, & Hassanien, A. E. (2018). Modified cuckoo search algorithm with rough sets for feature selection. *Neural Computing and Applications*, *29*(4), 925–934. https://doi.org/10.1007/s00521-016-2473-7

Balasaraswathi, V. R., Sugumaran, M., & Hamid, Y. (2017). Feature selection techniques for intrusion detection using non-bio-inspired and bio-inspired optimization algorithms. *Journal of Communications and Information Networks*, *2*(4), 107–119. https://doi.org/10.1007/s41650-017-0033-7

Benmessahel, I., Xie, K., & Chellal, M. (2017a). A new evolutionary neural networks based on intrusion detection systems using multiverse optimization. *Applied Intelligence*, 1–13.

Benmessahel, I., Xie, K., & Chellal, M. (2017b). A new evolutionary neural networks based on intrusion detection systems using multiverse optimization. *Applied Intelligence*. Retrieved from https://link.springer.com/article/10.1007/s10489-017-1085-y

Benmessahel, I., Xie, K., & Chellal, M. (2019). A new evolutionary neural networks based on intrusion detection systems using locust swarm optimization. *Applied Intelligence*, *48*(8), 2315–2327. https://doi.org/10.1007/s10489-017-1085-y

Benmessahel, I., Xie, K., Chellal, M., & Semong, T. (2019). A new evolutionary neural networks based on intrusion detection systems using locust swarm optimization. *Evolutionary Intelligence*, *12*(2), 131–146. https://doi.org/10.1007/s12065-019-00199-5

Cahyo, A. N., Hidayat, R., & Adhipta, D. (2016). Performance comparison of intrusion detection system based anomaly detection using artificial neural network and support vector machine. *International Journal for Research in Applied Science and Engineering Technology*, *1755*(2016). https://doi.org/10.1063/1.4958506

Carbonell, J. G., & Mitchell, T. M. (1983). AN OVERVIEW OF MACHINE LEARNING. In *MACHINE LEARNING: An Artificial Intelligence Approach*. https://doi.org/10.1016/B978-0-08-051054-5.50005-4

Cateni, S., Colla, V., & Vannucci, M. (2017). A hybrid feature selection method for classification purposes. *Proceedings - UKSim-AMSS 8th European Modelling Symposium on Computer Modelling and Simulation*, (October), 39–44. https://doi.org/10.1109/EMS.2014.44

Chandrashekhar, A. ., & Raghuveer. (2013). Fortification of Hybrid Intrusion Detection System Using Variants of Neural Networks and Support Vector Machines. *International Journal of Network Security & Its Applications*, *5*(1), 71–90. https://doi.org/10.5121/ijnsa.2013.5106

Chiba, Z., Abghour, N., Moussaid, K., El omri, A., & Rida, M. (2019). Intelligent and improved self-adaptive anomaly based intrusion detection system for networks. *International Journal of Communication Networks and Information Security*, *11*(2), 312–330.

Corne, D., & Lones, M. A. (2018). Evolutionary algorithms. *Handbook of Heuristics Natural Computing Series Book Series (NCS), 1–2*, 409–430. https://doi.org/10.1007/978-3-319-07124-4_27

Cowan, J. D. (1990). Discussion: McCulloch-Pitts and related neural nets from 1943 to 1989. *Bulletin of Mathematical Biology*, *52*(1–2), 73–97. https://doi.org/10.1007/BF02459569

Dastanpour, A., & Mahmood, R. A. R. (2013). Feature selection based on genetic algorithm and SupportVector machine for intrusion detection system. *International Informatics Engineering & Information Science*, (September 2014), 169–181. https://doi.org/10.13140/2.1.4289.4721

De Campos, L. M. L., De Oliveira, R. C. L., & Roisenberg, M. (2015). Evolving Artificial Neural Networks through L-system and evolutionary computation. *Proceedings of the International Joint on Neural Networks*, *2015-Septe*. https://doi.org/10.1109/IJCNN.2015.7280535

Denning, D. E. (1987). An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*, (2), 222–232.

Dhanabal, L., & 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), 446–452. https://doi.org/10.17148/IJARCCE.2015.4696

Dhanda, N., Datta, S. S., & Dhanda, M. (2019). Machine Learning Algorithms. *Journal of Communications and Information Networks*, (May), 210–233. https://doi.org/10.4018/978-1-5225-7955-7.ch009

Dias, L. P., Cerqueira, J. J. F., & Assis, K. D. R. (2017). Using Artificial Neural

Network in Intrusion Detection Systems to Computer Networks. *IEEE Transactions on Software Engineering*, 145–150.

Effendy, D. A., Kusrini, K., & Sudarmawan, S. (2017). Classification of intrusion detection system (IDS) based on computer network. *International Journal for Research in Applied Science and Engineering Technology*, *2018-Janua*, 90–94. https://doi.org/10.1109/ICITISEE.2017.8285566

Fajardo, S., García-Galvan, R., F., Barranco, V., Galvan, J. C., & Batlle, S. F. (2016). Anomaly-Based Intrusion Detection System. *Computer and Network Security*, *i*(tourism), 13. https://doi.org/http://dx.doi.org/10.5772/57353

Faris, H., Aljarah, I., & Mirjalili, S. (2016). Training feedforward neural networks using multi-verse optimizer for binary classification problems. *Applied Intelligence*, *45*(2), 322–332. https://doi.org/10.1007/s10489-016-0767-1

Faris, H., Hassonah, M. A., Al-Zoubi, A. M., Mirjalili, S., & Aljarah, I. (2018). A multi-verse optimizer approach for feature selection and optimizing SVM parameters based on a robust system architecture. *Neural Computing and Applications*, *30*(8), 2355–2369. https://doi.org/10.1007/s00521-016-2818-2

Feng, W., Zhang, Q., Hu, G., & Huang, J. X. (2014). Mining network data for intrusion detection through combining SVMs with ant colony networks. *Future Generation Computer Systems*, *37*, 127–140. https://doi.org/10.1016/j.future.2013.06.027

Ferguson, T. S. (1961). on the Rejection of Outliers. *In Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability (Vol. 1, No. 1, Pp. 253-287). Berkeley: University of California Press.*, *I*(05), 253–287.

Fu, T. C., & Lui, C. L. (2007). Agent-oriented network intrusion detection system using data mining approaches. *International Journal of Agent-Oriented Software Engineering*, *1*(2), 158–174. https://doi.org/10.1504/IJAOSE.2007.014403

Gayon, J. (2003). From Darwin to today in evolutionary biology. In *The Cambridge Companion to Darwin*. https://doi.org/10.1017/CCOL0521771978.011

Giridhar, M. S., Sivanagaraju, S., Suresh, C. V., & Umapathi Reddy, P. (2017). Analyzing the multi objective analytical aspects of distribution systems with multiple multi-type compensators using modified cuckoo search algorithm. *International Journal of Parallel, Emergent and Distributed Systems*, *32*(6), 549–571. https://doi.org/10.1080/17445760.2016.1173214

Hadri, A., Chougdali, K., & Touahni, R. (2016). Intrusion detection system using PCA and Fuzzy PCA techniques. *Australian Journal of Basic and Applied Sciences*, 1–7. https://doi.org/10.1109/ACOSIS.2016.7843930

Hajamydeen, A. I., & Udzir, N. I. (2019). A detailed description on unsupervised heterogeneous anomaly based intrusion detection framework. *Scalable Computing*, *20*(1), 113–160. https://doi.org/10.12694/scpe.v20i1.1465

He, D., Chen, X., Zou, D., Pei, L., & Jiang, L. (2018). An Improved Kernel Clustering Algorithm Used in Computer Network Intrusion Detection. *Proceedings - IEEE International Symposium on Circuits and Systems*, *2018-May*, 3–7. https://doi.org/10.1109/ISCAS.2018.8350994

Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2018). *A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets*. *1*(1). Retrieved from http://arxiv.org/abs/1806.03517

Hodo, E. and D. N. I. D. S. A. T. and S., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2017). *Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey*. 1–43. Retrieved from http://arxiv.org/abs/1701.02145

Hsiao, S., Mattox, S., Park, T., Selvaraj, S., & Tam, A. (2019). Anomaly Detection UsingSVM as Classifier and Decision Tree for Optimizing Feature Vectors. *The ISC Intl Journal of Information Security*.

Hu, C., Li, Z., Zhou, T., Zhu, A., & Xu, C. (2016). A multi-verse optimizer with levy flights for numerical optimization and its application in test scheduling for network-on-chip. *PLoS ONE*, *11*(12). https://doi.org/10.1371/journal.pone.0167341

Hu, L., Zhang, Z., Tang, H., & Xie, N. (2015). An Improved Intrusion Detection Framework Based on Artificial Neural Networks. *Security and Communication Networks*, *1*(2015), 887–890. https://doi.org/10.1109/ICICISYS.2009.5358048

Huang, G. Bin, Zhou, H., Ding, X., & Zhang, R. (2012). Extreme learning machine for regression and multiclass classification. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, *42*(2), 513–529. https://doi.org/10.1109/TSMCB.2011.2168604

Hussain, J., Lalmuanawma, S., & Chhakchhuak, L. (2016). A two-stage hybrid classification technique for network intrusion detection system. *International Journal of Computational Intelligence Systems*, *9*(5), 863–875. https://doi.org/10.1080/18756891.2016.1237186

Iqbal, A., & Aftab, S. (2019). A Feed-Forward and Pattern Recognition ANN Model for Network Intrusion Detection. *International Journal of Computer Network and Information Security*, *11*(4), 19–25. https://doi.org/10.5815/ijcnis.2019.04.03

Jangir, P., Parmar, S. A., Trivedi, I. N., & Bhesdadiya, R. H. (2017). A novel hybrid Particle Swarm Optimizer with multi verse optimizer for global numerical optimization and Optimal Reactive Power Dispatch problem. *Engineering Science and Technology, an International Journal*, *20*(2), 570–586. https://doi.org/10.1016/j.jestch.2016.10.007

Jawhar, M. M. T., & Mehrotra, M. (2010). Design Network Intrusion Detection System using hybrid Fuzzy-Neural Network. *International Journal of Computer*

Science and Security, *4*(3), 285–294.

Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. (2018). A Survey on Anomaly Based Host Intrusion Detection System. *Journal of Physics and Science*, *1000*(1). https://doi.org/10.1088/1742-6596/1000/1/012049

Joshi, A. S., Kulkarni, O., Kakandikar, G. M., & Nandedkar, V. M. (2017). Cuckoo Search Optimization- A Review. *Materials Today: Proceedings*, *4*(8), 7262–7269. https://doi.org/10.1016/j.matpr.2017.07.055

Ke, G., & Hong, Y. H. (2014). The research of network intrusion detection technology based on genetic algorithm and BP neural network. *Applied Mechanics and Materials*, *599–601*, 726–730. https://doi.org/10.4028/www.scientific.net/AMM.599-601.726

Khalid, S., Khalil, T., & Nasreen, S. (2017). A survey of feature selection and feature extraction techniques in machine learning. *Procedia Computer Science*, 372–378. https://doi.org/10.1109/SAI.2014.6918213

Khari, M., Gupta, S., Shrivastava, G., & Gupta, R. (2017). Role of cyber security in today’s scenario. *Detecting and Mitigating Robotic Cyber Security Risks*, 177–191. https://doi.org/10.4018/978-1-5225-2154-9.ch013

Khraisat, A., Gondal, I., & Vamplew, P. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1). https://doi.org/10.1186/s42400-019-0038-7

Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, *41*(4 PART 2), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066

Kohavi, R., & John, G. H. (1997). Wrappers for feature subset selection. *Artificial Intelligence*, *97*(1–2), 273–324. https://doi.org/10.1016/s0004-3702(97)00043-x

Kuang, F., Xu, W., & Zhang, S. (2014). A novel hybrid KPCA and SVM with GA model for intrusion detection. *Applied Soft Computing Journal*, *18*, 178–184. https://doi.org/10.1016/j.asoc.2014.01.028

Kumar, P., & Kumar, S. (2017). Intrusion Detection Systems in Clustering: A Review. *International Journal for Research in Applied Science and Engineering Technology*, *V*(VIII), 2244–2249. https://doi.org/10.22214/ijraset.2017.8322

Le, T. T. H., Kim, Y., & Kim, H. (2019). Network intrusion detection based on novel feature selection model and various recurrent neural networks. *Applied Sciences (Switzerland)*, *9*(7). https://doi.org/10.3390/app9071392

Li, Y., Xia, J., & Zhang, S. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. *Expert Systems with Applications*, *39*(1), 424–430. https://doi.org/10.1016/j.eswa.2011.07.032

Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. *Expert Systems with Applications*, *39*(1), 424–430. https://doi.org/10.1016/j.eswa.2011.07.032

Li, Z., Rios, L. G., Xu, G., & Trajkovi´, L. (2019). Machine learning techniques for classifying network anomalies and intrusions. *Proceedings - IEEE International Symposium on Circuits and Systems*, *2019-May*, 1–5. https://doi.org/10.1109/ISCAS.2019.8702583

Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, *78*(1), 13–21. https://doi.org/10.1016/j.knosys.2015.01.009

Ludwig, S. A. (2019). Applying a Neural Network Ensemble to Intrusion Detection. *Journal of Artificial Intelligence and Soft Computing Research*, *9*(3), 177–188. https://doi.org/10.2478/jaiscr-2019-0002

Lunt, T. F., Jagannathan, R., Lee, R., Whitehurst, A., & Listgarten, S. (1980). Knowledge-based intrusion detection. *International Information Security*, 102–107. https://doi.org/10.1109/aisig.1989.47311

Ma, J., & Perkins, S. (2003). Online novelty detection on temporal sequences. *ACM SIGKDD Knowledge Discovery and Data Mining*, 613–618. https://doi.org/10.1145/956750.956828

Mahmood, D. I., & Hameed, S. M. (2016). A Feature Selection Model based on Genetic Algorithm for Intrusion Detection. *Iraqi Journal of Science*, (April), 168–175. https://doi.org/10.1177/1045389X14554132

Mamatha, G. S., & Sharma, S. C. (2010). A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS. *International Journal of Computer Science and Security (IJCSS)*, *4*(3), 275.

Masduki, B. W., Ramli, K., Saputra, F. A., & Sugiarto, D. (2015). Study on implementation of machine learning methods combination for improving attacks detection accuracy on Intrusion Detection System (IDS). *Computers and Electrical Engineering*, 56–64. https://doi.org/10.1109/QiR.2015.7374895

Meshkat, M., & Parhizgar, M. (2017). Stud Multi-Verse Algorithm. *IEEE Transactions on Parallel and Distributed Systems*, 42–47. https://doi.org/10.1109/CSIEC.2017.7940155

Miao, J., & Niu, L. (2017). A Survey on Feature Selection. *Procedia Computer Science*, *91*(Itqm), 919–926. https://doi.org/10.1016/j.procs.2016.07.111

Min, E., Long, J., Liu, Q., Cui, J., & Chen, W. (2018). TR-IDS: Anomaly-Based Intrusion Detection through Text-Convolutional Neural Network and Random Forest. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/4943509

Min, H., & Fangfang, W. (2010). Filter-wrapper hybrid method on feature selection. *Proceedings - 2010 2nd WRI Global Congress on Intelligent Systems, GCIS 2010*, *3*, 98–101. https://doi.org/10.1109/GCIS.2010.235

Mirjalili, S., Jangir, P., Mirjalili, S. Z., Saremi, S., & Trivedi, I. N. (2017). Optimization of problems with multiple objectives using the multi-verse optimization algorithm. *Knowledge-Based Systems*, *134*, 50–71. https://doi.org/10.1016/j.knosys.2017.07.018

Mirjalili, S., Mirjalili, S. M., & Hatamlou, A. (2016). Multi-Verse Optimizer: a nature-inspired algorithm for global optimization. *Neural Computing and Applications*, *27*(2), 495–513. https://doi.org/10.1007/s00521-015-1870-7

Mocller, R. R. (2018). Network security: IDS/SIEM. *Information Systems Security*, *2*(1), 30–32. https://doi.org/10.1080/19393559308551341

Mohammadi, S., Mirvaziri, H., Ghazizadeh-Ahsaee, M., & Karimipour, H. (2019). Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and Applications*, *44*, 80–88. https://doi.org/10.1016/j.jisa.2018.11.007

Najeeb, R. F., & Dhannoon, B. N. (2018). A feature selection approach using binary Firefly Algorithm for network intrusion detection system. *ARPN Journal of Engineering and Applied Sciences*, *13*(6), 2347–2352.

Napiah, M. N., Bin Idris, M. Y. I., Ramli, R., & Ahmedy, I. (2018a). Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol. *IEEE Access*, *6*, 16623–16638. https://doi.org/10.1109/ACCESS.2018.2798626

Napiah, M. N., Bin Idris, M. Y. I., Ramli, R., & Ahmedy, I. (2018b). Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol. *IEEE Access*, *6*(c), 16623–16638. https://doi.org/10.1109/ACCESS.2018.2798626

Nikhitha, M., & Jabbar, M. A. (2019). K Nearest Neighbor Based Model for Intrusion Detection System. *International Journal of Recent Technology and Engineering*, *8*(2), 2258–2262. https://doi.org/10.35940/ijrte.b2458.078219

Nolan, D. R., & Lally, C. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *24*(March), 132–142. https://doi.org/10.1016/j.jocs.2017.04.009

Nwankpa, C., Ijomah, W., Gachagan, A., & Marshall, S. (2018). *Activation Functions: Comparison of trends in Practice and Research for Deep Learning*. 1–20. Retrieved from http://arxiv.org/abs/1811.03378

Omran, M. G. H., Engelbrecht, A. P., & Salman, A. (2007). An overview of clustering methods. *Intelligent Data Analysis*, *11*(6), 583–605.

https://doi.org/10.9790/3021-0204719725

Ouaarab, A., Ahiod, B., & Yang, X. S. (2014). Discrete cuckoo search algorithm for the travelling salesman problem. *Neural Computing and Applications*, *24*(7–8), 1659–1669. https://doi.org/10.1007/s00521-013-1402-2

Pan, W., Li, Z., & Zhou, Y. (2017). An exponential function inflation size of multi-verse optimisation algorithm for global optimisation. *International Journal of Computing Science and Mathematics*, *8*(2), 115. https://doi.org/10.1504/ijcsm.2017.10004514

Pentapalli, V. G., Varma, V. K., & Ravi, P. (2016). Cuckoo Search Optimization and its Applications: A Review. *International Journal of Advanced Research in Computer and Communication Engineering ISO*, *3297*(11), 556–562. https://doi.org/10.17148/IJARCCE.2016.511119

Protić, D. (2018). Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ datasets. *Vojnotehnicki Glasnik*, *66*(3), 580–596. https://doi.org/10.5937/vojtehg66-16670

Qiu, C., & Shan, J. (2015). Research on intrusion detection algorithm based on BP neural network. *International Journal of Security and Its Applications*, *9*(4), 247–258. https://doi.org/10.14257/ijsia.2015.9.4.23

Rai, K., Devi, M. S., & Guleria, A. (2016). Decision Tree Based Algorithm for Intrusion Detection. *International Journal of Advanced Networking and Applications*, *07*(04), 2828–2834. Retrieved from https://www.researchgate.net/publication/298175900

Resende, P. A. A., & Drummond, A. C. (2018). Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling. *Security and Privacy*, *1*(4), e36. https://doi.org/10.1002/spy2.36

Roopa Devi, E. M., & Suganthe, R. C. (2018). Enhanced transductive support vector machine classification with grey wolf optimizer cuckoo search optimization for intrusion detection system. *Concurrency Computation* , (July), 1–11. https://doi.org/10.1002/cpe.4999

S´anchez-Maro˜no, N., Alonso-Betanzos, A., & Tombilla-Sanrom´an, M. (2007). Filter methods for feature selection. A comparative study. *Ideal*, *4881*(December), 790–799. https://doi.org/10.1007/978-3-540-77226-2

Sangkatsanee, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2011). Practical real-time intrusion detection using machine learning approaches. *Computer Communications*, *34*(18), 2227–2235. https://doi.org/10.1016/j.comcom.2011.07.001

Sarvari, S., Muda, Z., Ahmad, I., & Barati, M. (2015). GA and SVM algorithms for selection of hybrid feature in intrusion detection systems. *International Review on Computers and Software*, *10*(3), 265–270. https://doi.org/10.15866/irecos.v10i3.5180

Sayed, G. I., Darwish, A., & Hassanien, A. E. (2017). Quantum multiverse optimization algorithm for optimization problems. *Neural Computing and Applications*, 1–18. https://doi.org/10.1007/s00521-017-3228-9

Sayed, G. I., Darwish, A., & Hassanien, A. E. (2018). A new chaotic multi-verse optimization algorithm for solving engineering optimization problems. *Journal of Experimental and Theoretical Artificial Intelligence*, *30*(2), 293–317. https://doi.org/10.1080/0952813X.2018.1430858

Schmidt, W. F., Kraaijveld, M. A., & Duin, R. P. W. (1992). Feed forward neural networks with random weights. *Proceedings - International Conference on Pattern Recognition*, *2*(July), 1–4. https://doi.org/10.1109/ICPR.1992.201708

Selvakumar, B., & Muneeswaran, K. (2019). Firefly algorithm based feature selection for network intrusion detection. *Computers and Security*, *81*, 148–155. https://doi.org/10.1016/j.cose.2018.11.005

Sen, N., Sen, R., & Chattopadhyay, M. (2014). An effective back propagation neural network architecture for the development of an efficient anomaly based intrusion detection system. *Security and Communication Networks*, 1052–1056. https://doi.org/10.1109/CICN.2014.221

Shafi, K., & Abbass, H. A. (2009). An adaptive genetic-based signature learning system for intrusion detection. *Expert Systems with Applications*, *36*(10), 12036–12043. https://doi.org/10.1016/J.ESWA.2009.03.036

Shanmugavadivu, R., & Nagarajan, D. N. (2018). Network intrusion detection system using fuzzy logic. *Indian Journal of Computer Science and Engineering*, *2*(1), 101–111. Retrieved from http://www.ijcse.com/docs/IJCSE11-02-01-034.pdf

Shehab, M., Khader, A. T., & Al-Betar, M. A. (2017). A survey on applications and variants of the cuckoo search algorithm. *Applied Soft Computing Journal*, *61*, 1041–1059. https://doi.org/10.1016/j.asoc.2017.02.034

Shen, Z., Zhang, Y., & Chen, W. (2019). A Bayesian Classification Intrusion Detection Method Based on the Fusion of PCA and LDA. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/6346708

Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. *ICT Express*, *4*(2), 95–99. https://doi.org/10.1016/j.icte.2018.04.003

Shilpashree, S., Lingareddy, S. C., Bhat, N. G., & Kumar, G. (2019). Decision tree: A machine learning for intrusion detection. *International Journal of Innovative Technology and Exploring Engineering*, *8*(6 Special Issue 4), 1126–1130. https://doi.org/10.35940/ijitee.F1234.0486S419

Sivatha Sindhu, S. S., Geetha, S., & Kannan, A. (2012). Decision tree based light weight intrusion detection using a wrapper approach. *Expert Systems with Applications*, *39*(1), 129–141. https://doi.org/10.1016/j.eswa.2011.06.013

Solomon, I. A., Jatain, A., & Bajaj, S. B. (2019). Neural Network Based Intrusion Detection: State of the Art. *SSRN Electronic Journal*, 1390–1396. https://doi.org/10.2139/ssrn.3356505

Su, M. Y. (2011). Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers. *Expert Systems with Applications*, *38*(4), 3492–3498. https://doi.org/10.1016/j.eswa.2010.08.137

Subba, B., Biswas, S., & Karmakar, S. (2016a). A Neural Network based system for Intrusion Detection and attack classification. *International Journal of Computer Applications*, 1–6. https://doi.org/10.1109/NCC.2016.7561088

Subba, B., Biswas, S., & Karmakar, S. (2016b). Enhancing performance of anomaly based intrusion detection systems through dimensionality reduction using principal component analysis. *International Journal of Network Security*, (August 2017). https://doi.org/10.1109/ANTS.2016.7947776

Sulaiman, M. H., Mustaffa, Z., Mohamed, M. R., & Aliman, O. (2017). An application of multi-verse optimizer for optimal reactive power dispatch problems. *International Journal of Simulation: Systems, Science and Technology*, *17*(41), 5.1-5.5. https://doi.org/10.5013/IJSSST.a.17.41.05

Swisscom. (2019). *Targeted Attacks Cyber Security Report 2019*. 34. Retrieved from https://www.swisscom.ch/content/dam/swisscom/de/about/unternehmen/portraet/netz/sicherheit/documents/security-report-2019.pdf.res/security-report-2019.pdf

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009*, (July). https://doi.org/10.1109/CISDA.2009.5356528

Thakkar, A., & Lohiya, R. (2020). Role of swarm and evolutionary algorithms for intrusion detection system: A survey. *Swarm and Evolutionary Computation*, *53*(December 2019), 100631. https://doi.org/10.1016/j.swevo.2019.100631

Vaidyanathan, N. (2018). Machine learning More science than fiction. *Компьютерные Инструменты В Образовании*, (4).

Viegas, E. K., Santin, A. O., & Oliveira, L. S. (2017). Toward a reliable anomaly-based intrusion detection in real-world environments. *Computer Networks*, *127*, 200–216. https://doi.org/10.1016/j.comnet.2017.08.013

Wang, G., Hao, J., Mab, J., & Huang, L. (2010a). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. *Expert Systems with Applications*, *37*(9), 6225–6232. https://doi.org/10.1016/j.eswa.2010.02.102

Wang, G., Hao, J., Mab, J., & Huang, L. (2010b). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. *Expert Systems* *with Applications*, *37*(9), 6225–6232. https://doi.org/10.1016/j.eswa.2010.02.102

Wang, S., Jiang, Y., Chung, F., & Qian, P. (2015). Feedforward kernel neural networks, generalized least learning machine, and its deep learning with application to image classification. *Applied Soft Computing Journal*, 1–17. https://doi.org/10.1016/j.asoc.2015.07.040

Wang, Y., Velswamy, K., & Huang, B. (2018). A Novel Approach to Feedback Control with Deep Reinforcement Learning□. *IFAC-PapersOnLine*, *51*(18), 31–36. https://doi.org/10.1016/j.ifacol.2018.09.241

Xiang, C., Yong, P. C., & Meng, L. S. (2008). Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees. *Pattern Recognition Letters*, *29*(7), 918–924. https://doi.org/10.1016/j.patrec.2008.01.008

Xingzhu, W. (2015). ACO and SVM selection feature weighting of network intrusion detection method. *International Journal of Security and Its Applications*, *9*(4), 259–270. https://doi.org/10.14257/ijsia.2015.9.4.24

Xu, B., Chen, S., Zhang, H., & Wu, T. (2017). Incremental k-NN SVM method in intrusion detection. *Security and Communication Networks*, *2017-Novem*, 712–717. https://doi.org/10.1109/ICSESS.2017.8343013

Xu, X., Liu, H., & Yao, M. (2019). Recent Progress of Anomaly Detection. *Complexity*, *2019*. https://doi.org/10.1155/2019/2686378

Yang, X., Cb, C., & Deb, S. (2009). Cuckoo Search via L ´ evy Flights. *IEEE Publications,USA,Pp*. https://doi.org/arXiv:1003.1594v1

Yao, X. (1993). A Review of Evolutionary Artifcial Neural Network. *International Journal of Intelligent Systems*.

Zainaddin, D. A. A., & Hanapi, Z. M. (2013). Hybrid of fuzzy clustering neural network over NSL dataset for intrusion detection system. *Journal of Computer Science*, *9*(3), 391–403. https://doi.org/10.3844/jcssp.2013.391.403

Zhao, Y., Zhao, Y., & Zhao, X. (2013). Network Intrusion Detection Based on IPSO-BPNN. *Information Technology Journal*.

Zhou, Yongquan, & Zheng, H. (2013). A Novel Complex Valued Cuckoo Search Algorithm. *The Scientific World Journal*, *2013*(1), 1–6. https://doi.org/10.1155/2013/597803

Zhou, Yuyang, Cheng, G., Jiang, S., & Dai, M. (2019). *An Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier*. (December), 0–12. Retrieved from http://arxiv.org/abs/1904.01352