METAHEURISTIC-BASED NEURAL NETWORK TRAINING AND FEATURE SELECTOR FOR INTRUSION DETECTION

WAHEED ALI HUSSEIN MOHAMMED GHANEM

UNIVERSITI SAINS MALAYSIA
2019

METAHEURISTIC-BASED NEURAL NETWORK TRAINING AND FEATURE SELECTOR FOR INTRUSION DETECTION

by

WAHEED ALI HUSSEIN MOHAMMED GHANEM

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

April 2019

DECLARATION

Name: Waheed Ali Hussein Mohammed Ghanem.

Matric No: P-COD0002/14.

Faculty: School of Computer Sciences.

Thesis Title: METAHEURISTIC-BASED NEURAL NETWORK TRAINING AND FEATURE SELECTOR FOR INTRUSION DETECTION.

I hereby declare that this thesis in I have submitted to School of Computer Sciences on 1/4/2019 is my own work. I have stated all references used for the completion of my thesis.

I agree to prepare electronic copies of the said thesis to the external examiner or internal examiner for the determination of amount of words used or to check on plagiarism should a request be made.

I make this declaration with the believe that what is stated in this declaration is true and the thesis as forwarded is free from plagiarism as provided under Rule 6 of the Universities and University Colleges (Amendment) Act 2008, University Science Malaysia Rules (Student Discipline) 1999.

I conscientiously believe and agree that the University can take disciplinary actions against me under Rule 48 of the Act should my thesis be found to be the work or ideas of other persons.

Student's Signature: Date: 1/4/2019

Acknowledgement of receipt by: Date:

ACKNOWLEDGEMENT

First of all, I would like to thank the Almighty Allah for giving me the strength, patience and ability to complete this thesis.

I would like to express my deep sense of thanks to my supervisor **Associate Professor Dr. AMAN B. JANTAN**, for his thoughtful comments, guidance, attention and encouragement. Furthermore, I would like to thank him for the invaluable advice and assistance and for the idea of the thesis in the first place.

I would like extend my sincere appreciations to my friend Ahmed for the continuous aid in every aspect, academic and otherwise. Also, I thank my friend Zahir, as he generously gave me very good advices. I would like to extend my grateful appreciation to all those who have contributed directly or indirectly to the completion of this study.

I would also like to thank my Parents for their love and support throughout my entire life, also I would like to thank my brothers for their encouragement. Special thanks go to my beloved wife for all support, patience, understanding and being helpful throughout my study. Moreover, deep thanks to my children Ali, Sundus, Sama, Ahmed and Laith for their inspiration during my research work. The successful completion of my work is the fruit of their sacrifices, devotion, and determination.

Finally, special thanks to the Institute of Postgraduate Studies (IPS) for granting me the USM Fellowship. This financial support is just one of the many merits that USM have provided for its students.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATONS

ABC	Artificial Bee Colony Algorithm
ACC	Accuracy
ACO	Ant Colony Optimization Algorithm
AD	Anomaly Detection
AFSA	Artificial Fish Swarm Algorithm
AI	Artificial Intelligence
ALO	Ant Lion Optimizer
AMGA	Multi Objective Genetic Algorithm
ANN	Artificial Neural Network
BA	Bees algorithm
BAR	Butterfly Adjusting Rate
BAT	Bat Algorithm
BBO	Biogeography Based Optimization Algorithm
BCO	Bee Colony Optimization
BP	Back-Propagation
BPNN	Back Propagation Neural Network
CEP	Classification Error Percentage
CFA	Cuttlefish Algorithm
CI	Computational Intelligence
CID	Intrusion Detection Capability
CS	Cuckoo Search Algorithm
CSI	Computational Swarm Intelligence
DA	Dragonfly Algorithm
DE	Differential Evolution Algorithm
DM	Detection Method
DOS	Denial Of Service

DR	Detection Rate
DT	Decision Tree
EA	Evolutionary Algorithm
EBAT	Enhanced Bat Algorithm
EC	Evolutionary Computation
EHO	Elephant Herding Optimization
ENN	Evolutionary Neural Network
ES	Evolution Strategy Algorithm
EWA	Earthworm Optimization Algorithm
FAR	False Alarm Rate
FFNN	Feed-Forward Neural Network
FN	False Negative
FNN	Fuzzy Neural Network
FP	False Positive
FS	Feature Selection
FSM	Feature Selection Method
GA	Genetic Algorithm
GDA	Great Deluge Algorithm
GHSOM	Growing Hierarchical Self-Organising Map
GQPSO	Genetic Quantum Particle Swarm Optimization
GSA	Gravitational Search Algorithm
GWO	Grey Wolf Optimizer Algorithm
HAD	Hybrid Artificial Bee Colony/Dragonfly Algorithm
HAM	Hybrid Artificial Bee Colony/Monarch Butterfly
HbPHAD	Host-based Packet Header Anomaly Detection
HG	Hypergraph
HIDS	Host Based Intrusion Detection System

HS	Harmony Search Algorithm
ID	Intrusion Detection
IDES	Intrusion Detection Expert System
IDS	Intrusion Detection System
IG	Information Gain
IP	Internet Protocol
IPS	Intrusion Prevention System
KH	Krill herd Algorithm
KMC	K-Means Clustering
K-SVCR	K-Support Vector Classification-Regression
LGP	Linear Genetic Programming
LM	Levenberg-Marquardt
LR	Logistic Regression
LSE	Least Square Error
MARS	Multivariate Regression Splines
MBO	Monarch Butterfly Optimization
MCLP	Multiple Criteria Linear Programming
MD	Misuse Detection
MFO	Moth-Flame Optimization
MGSA	Modified Gravitational Search Algorithm
MLFFNN	Multi-Layer Feed Forward Neural Network
MLP	Multi-Layer Perceptron
MNN	Modular Neural Network
MOEA/D	Multi-Objective Evolutionary Algorithm with Decomposition
MOO	Multi-Objective Optimization
MPPSO	Multi-Objective Particle Swarm Optimization

MQPSO	Modified Quantum-Behaved Particle Swarm Optimization
MSA	Moth Search Algorithm
MSE	Mean Square Error
MVO	Multi-Verse Optimizer
NB	Naïve Bayes
NBC	Naïve Bayes Classifier
NBTree	Naïve Bayes Tree
NIDS	Network Based Intrusion Detection System
NNC	Nearest Neighbor Classifier
NSGA	Non-dominated Sorting Genetic Algorithm
PBIL	Probability-Based Incremental Learning
PCA	Principle Component Analysis
PCCE	Percentage of Correctly Classified Example
PSO	Particle Swarm Optimization
QPSO	Quantum-behaved Particle Swarm Optimization
RBF	Radial Basis Function
RBFNN	Radial Basis Function Neural Network
REPTree	Reduced Error Pruning Tree Algorithm
RF	Random Forest
RFA	Recursive Feature Addition
RMSE	Root-Mean-Square Error
RNN	Recurrent Neural Network
SCA	Sine Cosine Algorithm
SGO	Stochastic Global Optimization
SI	Swarm Intelligence
SN	Solution Number
SSE	Sum of Square Error

StudGA	StudGA Genetic Algorithm
SVDF	Support Vector Decision Function
SVM	Support Vector Machine
TCP	Transmission Control Protocol
TMAD	Text Mining-based Anomaly Detection
TN	True Negative
TP	True Positive
TVCPSO	Time-Varying Chaos Particle Swarm Optimization
UDP	User Datagram Protocol
WFNN	Wavelet Fuzzy Neural Network
WNN	Wavelet Neural Network
WOA	Whale Optimization Algorithm

LATIHAN RANGKAIAN NEURAL DAN PEMILIH CIRI BERASAKAN METAHEURISTIK UNTUK PENGESANAN PENCEROBOHAN

ABSTRAK

Pengesanan Pencerobohan dalam konteks rangkaian komputer merupakan teknik penting dalam strategi pertahanan keselamatan mendalam yang moden. Sistem Pengesanan Pencerobohan mendapat perhatian yang luar biasa daripada penyelidik dan pakar keselamatan. Konsep penting dalam pengesanan pencerobohan adalah pengesanan anomali yang merupakan pengasingan normal dalam trafik rangkaian daripada peristiwa tidak normal (anomali). Pengasingan ini pada asasnya merupakan tugas klasifikasi, yang menyebabkan penyelidik cuba untuk menggunakan pengklasifikasi terkenal dalam bidang pembelajaran mesin dalam pengesanan pencerobohan. Rangkaian saraf (NN) adalah salah satu teknik yang paling popular untuk melakukan klasifikasi bukan linear, dan digunakan secara meluas dalam kajian lepas untuk melakukan pengesanan pencerobohan. Pertama, dataset latihan biasanya menghasilkan set ciri maklumat yang tidak relevan atau berlebihan, yang menjejaskan prestasi klasifikasi. Kedua, algoritma pembelajaran tradisional seperti *backpropagation* mengalami masalah yang belum diatasi (known issue), termasuk penumpuan lambat dan perangkap untuk *local minimum*. Masalah-masalah tersebut menjejaskan proses pengoptimuman. Memandangkan kaedah *swarm intelligence* menghasilkan kejayaan besar dalam hal pengoptimuman, matlamat utama tesis ini adalah untuk menyumbangkan peningkatan teknologi pengesanan pencerobohan menerusi penggunaan teknik pengoptimuman berasaskan “swarm” dalam masalah asas pemilihan ciri paket yang optimum, dan latihan rangkaian saraf yang optimum untuk mengklasifikasikan ciri-ciri tersebut sebagai hal biasa dan serangan. Untuk

merealisasikan matlamat ini, penyelidikan dalam tesis ini mengikuti tiga peringkat asas, diikuti oleh penilaian yang meluas. Pertama, kajian ini bermula dengan mencari algoritma metaheuristik yang sesuai dan boleh digunakan untuk melatih rangkaian saraf bagi tujuan Pengesanan Pencerobohan. Carian ini mengakibatkan pembangunan tiga algoritma metaheuristik baharu: EBAT (Enhanced Bat Algorithm), yang mengubah algoritma BAT klasik untuk prestasi yang lebih baik; Algoritma HAM (Hybrid Artificial Bee Colony and Monarch Butterfly); dan Algoritma HAD (Hybrid Artificial Bee Colony and Dragonfly). Kedua, tiga algoritma yang dicadangkan itu digunakan untuk latihan MLP. Aplikasi algoritma ini dalam tugas latihan rangkaian saraf untuk pengesanan pencerobohan dinilai secara meluas dan prestasinya dibandingkan dengan metaheuristik tradisional dan yang terkini. Ketiga, algoritma BAT versi binari dicadangkan sebagai kaedah pengoptimuman multiobjektif baharu untuk memilih set ciri yang optimum untuk mengklasifikasikan paket rangkaian. Komponen asas terdahulu menghasilkan sistem pengesanan pencerobohan yang berkesan dan cekap, yang dinilai pada dataset yang standard seperti KDD Cup 1999, NSL KDD, ISCX2012 dan UNSW NB15, serta dibandingkan dengan pendekatan alternatif yang sama daripada kajian lepas. Teknik yang dicadangkan menunjukkan kelebihan yang konsisten merentasi dataset yang berbeza berbanding dengan teknik lain. Secara khususnya, ketepatan keseluruhan purata, kadar penggera palsu dan kadar pengesanan masing-masing adalah 98.05, 0.0285 dan 99.59 berbanding KDD CUP'99, iaitu 99.16, 0.0148 dan 99.38 masing-masing, berbanding NSLKDD, iaitu 99.96, 0.0003 dan 99.95 masing-masing, berbanding ISCX2012 dan 97.63, 0.0326 dan 98.18 masing-masing, berbanding UNSW-NB15.

METAHEURISTIC-BASED NEURAL NETWORK TRAINING AND FEATURE SELECTOR FOR INTRUSION DETECTION

ABSTRACT

Intrusion Detection (ID) in the context of computer networks is an essential technique in modern defense-in-depth security strategies. As such, Intrusion Detection Systems (IDSs) have received tremendous attention from security researchers and professionals. An important concept in ID is anomaly detection, which amounts to the isolation of normal behavior of network traffic from abnormal (anomaly) events. This isolation is essentially a classification task, which led researchers to attempt the application of well-known classifiers from the area of machine learning to intrusion detection. Neural Networks (NNs) are one of the most popular techniques to perform non-linear classification, and have been extensively used in the literature to perform intrusion detection. However, the training datasets usually compose feature sets of irrelevant or redundant information, which impacts the performance of classification, and traditional learning algorithms such as backpropagation suffer from known issues, including slow convergence and the trap of local minimum. Those problems lend themselves to the realm of optimization. Considering the wide success of swarm intelligence methods in optimization problems, the main objective of this thesis is to contribute to the improvement of intrusion detection technology through the application of swarm-based optimization techniques to the basic problems of selecting optimal packet features, and optimal training of neural networks on classifying those features into normal and attack instances. To realize these objectives, the research in this thesis follows three basic stages, succeeded by extensive evaluations. First, this work starts by the search for suitable metaheuristic algorithms that can be used to train

neural networks for the purpose of ID. This search resulted in the development of three new metaheuristic algorithms: EBAT (Enhanced Bat Algorithm), which modifies the classic BAT algorithm for better performance; HAM (Hybrid Artificial Bee Colony and Monarch Butterfly) algorithm; and HAD (Hybrid Artificial Bee Colony and Dragonfly) algorithm. Second, the three proposed algorithms are adopted for MLPs training. The application of these algorithms to the task of training neural networks for intrusion detection is extensively evaluated and their performances are compared with other traditional as well as recent metaheuristics. Third, the binary version of the BAT algorithm is proposed as a new multi-objective optimization method to select the optimal feature set for classifying network packets. The previous basic components resulted in an effective and efficient intrusion detection system, which is evaluated on the standard KDD Cup 1999, NSL KDD, ISCX2012 and UNSW NB15 datasets, and compared with similar alternative approaches from the literature. The proposed technique showed consistent advantage across the different datasets over the other techniques. In particular, the average overall accuracy, false alarm rate and detection rate were 98.05, 0.0285 and 99.59, respectively against KDD CUP'99, 99.16, 0.0148 and 99.38, respectively against NSLKDD, 99.96, 0.0003 and 99.95, respectively against ISCX2012 and 97.63, 0.0326 and 98.18, respectively against UNSW-NB15.

CHAPTER ONE

INTRODUCTION

1.1 Overview

Protection of computer networks has been the target for a long list of network security technologies. This protection involves the defense against intrusions that may compromise the confidentiality, integrity, or availability of network resources (Merkow and Breithaupt, 2014; Mukhopadhyay et al., 2011; Patil et al., 2012). Despite their proliferation, individual technologies are still short of the full protection against network intrusions, and often several technologies are employed in a defense-in-depth setting. Among the most popular network security technologies are firewalls, Intrusion Prevention Systems (IPSs) and Intrusion Detection Systems (IDSs).

Firewalls are well-known mechanisms that control the access to network resources based on a predefined policy. Firewalls can separate large networks into many different zones and implement a different security policy for each zone. However, firewall technology cannot handle new attacks, and as such, it acts as the first line of defense against potential malicious actions, before intrusion detection systems (Akhyari and Fahmy, 2014; Ghorbani et al., 2009; Uddin and Hasan, 2016).

An IDS provides the network with a level of preventive security against any suspicious activity, via early warnings to systems administrators. Because intrusion detection systems are capable of detecting various types of malicious actions, they form an attractive second layer of network protection, which covers for the limitations of security policies in traditional firewalls (Amiri et al., 2014; Chowdhary et al., 2014).

The operation of IDSs can be summarized in the following operations: monitor, analyze, detect and stir alarms. An IDS can be classified into two types: network based IDS (NIDS), which detects cyber threats at the network level by evaluating network traffic; and host based IDS (HIDS), which detects the threats on individual computers or hosts within the network. IDSs use two methods for the detection: (1) misuse detection, which detects attacks using signature databases that contain signatures of known attacks, and (2) anomaly detection, which is based on the assumption that the behavior of the attacker is different than that of the mainstream user (c and Agrawal, 2012; Chadha and Jain, 2015).

Unlike an intrusion prevention system, an IDS is not designed to block attacks (Castro et al., 2013; Kim, G. et al., 2014). An IDS is a passive technique to monitor and warn on suspicious activities but cannot actively intervene and stop a potential attack. An IPS, on the other hand, is placed in-line along the traffic path between the firewall and the rest of the network, and can block the traffic in addition to sending alerts. In this sense, IPSs are extensions to IDSs, but they are too intrusive to the network operation that their deployment may not be preferred under current levels of accuracy and performance. Therefore, IDSs are more widely accepted and deployed. The sole focus of this thesis is the IDS technology.

1.2 Research Problem

Although IDSs are a mature technology, they still suffer from a fundamental problem, which is performance. Performance here refers to the rate of detecting actual threats while avoiding mistakes in reporting potential ones. The type of mistakes in which the system falsely reports an attack is known as false positives. The performance

of IDSs can be improved by increasing accurate detection rate and reducing the rate of false positives (Bahl and Sharma, 2015; Elhag et al., 2015).

An IDS that can handle new attacks must adopt an anomaly-detection strategy. This strategy is based on the premise that hostile behavior is different from normal user behavior, and by distinguishing abnormal activities, one can detect even new threats. This task is essentially a classification problem, which entails the training of a classifier model that employs a number of features to discriminate two or more classes in a given set of observations. Among the successful classifiers, artificial neural networks (ANNs) have been extensively used for the purpose of intrusion detection.

The problem with traditional ANN-based IDSs is twofold. On the one hand, the classifier's performance relies on a set of parameters. These parameters need to be learned until an optimal set of values is settled. In the case of ANNs, these parameters are a set of weights and biases that label network edges feeding into the nodes. Setting these weights is achieved by a training process that is in essence an optimization problem in which the space of all possible weights is searched looking for the optimal set of values that result in the best classification of network packets. Unfortunately, the search space of all weights is so large that the classic learning techniques, such as backpropagation, can only produce suboptimal values within the feasible time and computational resources. On the other hand, an IDS deals with huge amounts of data that contain irrelevant and redundant features, which leads to slow training and testing processes, higher resource consumption, and poor detection rates (Aghdam and Kabiri, 2016; Eesa et al., 2015a; Ravale et al., 2015; Zuech et al., 2015). Therefore, feature selection is a fundamental step in the design of an IDS. Optimized feature sets reduce the computational cost and time, improve the classification accuracy and decrease the false alarm rate.

Because training classifiers on a set of optimal parameters and selecting an optimal feature set are essentially optimization problems, metaheuristics emerge as a natural candidate solutions. This is especially true since traditional training techniques are based on the gradient descent algorithm, which is limited compared to metaheuristics that can be directly applied to an ANN. Several metaheuristics have already been attempted to train neural networks and address the problem of feature selection for intrusion detection and other applications. These metaheuristics span evolutionary computations (EC) such as the genetic algorithm and swarm intelligence such as particle swarm optimization. However, the nature of these algorithms leaves the room for much improvement since the most important challenge at the heart of any metaheuristic optimization algorithm is the ability to balance between the exploration and exploitation activities in the search space to find a global optimum solution. Nevertheless, the search for a proper exploration and exploitation trade-off remains a challenging task in any algorithm and can always be improved for a new application such as intrusion detection. This opportunity to find better metaheuristics to optimize IDS classifiers is the main driver of the research in this thesis.

This work builds on the premise that the limitations of existing feature selection and classification methods can be alleviated, and their performance can be improved, by exploiting metaheuristic-based optimization. This kind of optimization proved very effective in solving complex problems that involve numerous and changing variables. The sought optimization techniques can cover both the task of training the classifiers as well as the task of selecting an optimal set of features to perform classification. Besides, feature selection is a multi-objective problem that involves several objectives, leading to the need for multi-objective optimization, which is a major issue to be addressed in this research as well.

1.3 Research Motivation

The importance of intrusion detection systems has only been increasing as a crucial defense mechanism in the face of the ever-growing phenomenon of cyber-crime (Bitter et al., 2012; McGuire and Downling, 2013). Cyber-attacks are the new weapon used in electronic warfare around the world, and their impact extends well beyond personal or enterprise networks into governmental and critical national network. The latest Incident Statistics Report of the Malaysia Computer Emergency Response Team (MyCERT) shows that *intrusion* and *intrusion attempts* form the largest portion of reported incidents over the months from Jan-Dec 2017 (Figure 1.1). Figure 1.2 shows the total cyber incidents in 2017 (http://www.mycert.org.my).

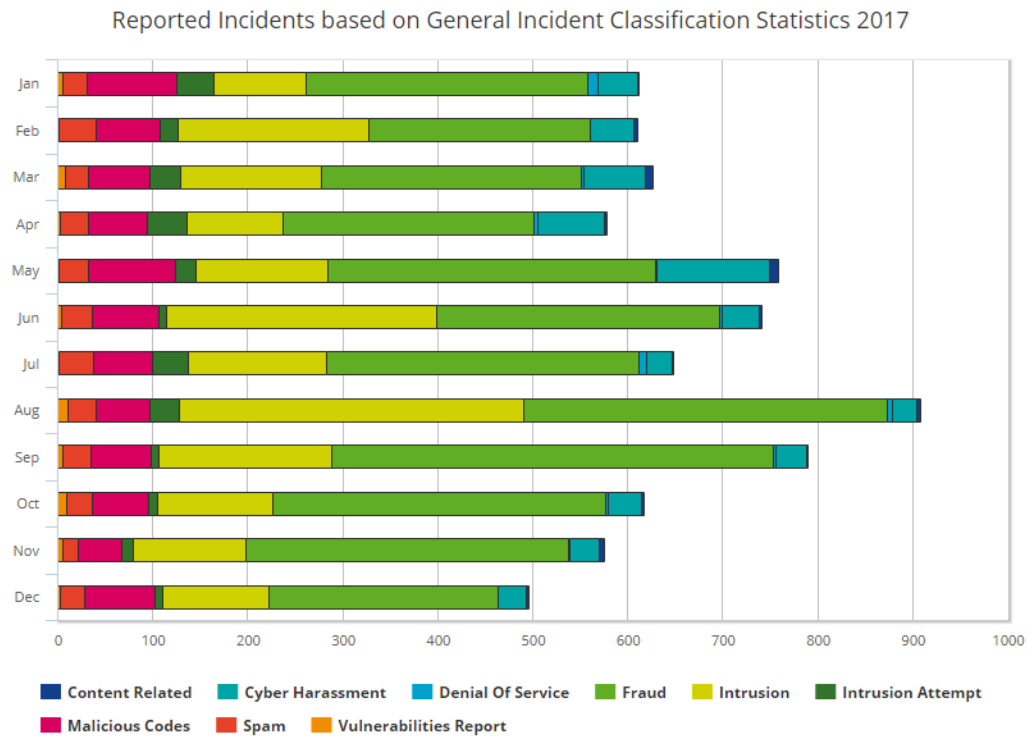

Figure 1.1: Reported incidents based on general incident classification statistics 2017 in Malaysia

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	5	9	2	9	2	1	4	2	2	5	3	46
Cyber Harassment	41	45	64	71	119	39	27	25	32	36	31	30	560
Denial of Service	11	0	3	3	1	3	8	6	2	2	1	0	40
Fraud	296	233	274	265	346	298	329	382	466	351	340	241	3821
Intrusion	98	201	148	101	138	284	146	363	181	121	119	111	2011
Intrusion Attempt	39	19	32	41	22	8	37	31	8	9	11	9	266
Malicious Code	94	68	65	62	92	71	62	56	64	60	46	74	814
Spam	26	38	24	30	31	32	36	30	29	26	17	25	344
Vulnerabilities Report	5	2	8	3	1	4	2	11	6	10	5	3	60
TOTAL	612	611	627	578	759	741	648	908	790	617	575	496	7962

Figure 1.2: Total cyber incidents from Jan to Dec 2017 in Malaysia

The phenomenal growth of cyber threats pushes security researchers and professionals into building more reliable protection mechanisms, including accurate IDS models that are capable of maximizing correctly detected threats and minimizing falsely detected threats at the same time. However, efficiency of the intrusion detection system is based mainly on features that are extracted from network traffic and an efficient and reliable classifier of traffic into normal or abnormal. This research further extends the search for an effective approach in that direction.

1.4 Research Question

Based on the research problem, available literature, and the goal of using metaheuristic-based optimization to improve the performance of intrusion detection models, the following research questions can be postulated:

1. How to improve the training of neural network models such that the learning algorithm can converge fast without trapping in local minima?

2. Can metaheuristic algorithms be used for training neural networks to produce the desired high accuracy over traditional learning algorithms?

3. If the answer to 2 is yes, what metaheuristic algorithm(s) can be used to train neural networks for the purpose of intrusion detection?

4. Does hybridization of metaheuristic algorithms produce better algorithms with high balance between exploration and exploitation processes? Does it improve the diversity and address the problems of local optima trapping?

5. If reducing the number of features entails multiple conflicting objectives, can multi-objective optimization be used for the extraction of the most relevant and non-duplicate features in order to build the intrusion detection model?

6. If the previous questions had been answered, how to combine a single-objective metaheuristic technique for training neural networks and a multi-objective metaheuristic for feature selection in a unified model of intrusion detection with the promised improved detection accuracy and reduced false alarm rate?

1.5 Research Goals and Objectives

The main goal of this research is to improve the performance of intrusion detection system on computer networks. This research proposes a detection approach that can address the deficit of existing intrusion detection systems. It extracts the important features of the network packets using a multi-objective optimization approach as a first step. The second step is to train a machine learning model using the enhanced metaheuristic algorithm, which can detect known and unknown attacks based on the features obtained from the previous step.

This overall objective can be broken into the following list of detailed objectives:

1. To design and develop a metaheuristic technique that can be used to improve the performance of training neural networks for the purpose of IDS. The developed

technique is to show better convergence and fitness accuracy for solving single and constrained-objective optimization problems.

2. To adapt the developed algorithm for the supervised training of Multi-Layer Perceptrons (MLPs). The proposed training method would incorporate suitable data representation and suitable fitness measure for classification applications.
3. To design and implement a new intrusion detection approach that utilizes the capabilities of the proposed multi-objective binary bat algorithm (MOBBAT) for wrapper-based feature selection to select an optimal set of features from network packets as a first stage. The second stage passes these features into the best MLP model from objective 2 for the detection of intrusions in the network.

The mapping between research questions (RQ), research objectives (RO), and research contributions (RC) of this research is summarized in Table 1.1 and Figure 1.3.

The first four questions led to the development of three new metaheuristic algorithms in the search for suitable metaheuristic trainer of neural networks (these algorithms are named EBAT, HAM and HAD).

The adaption of these algorithm to the training of neural networks for the purpose of intrusion detection resulted in three corresponding training algorithms: EBATMPL, HAMMPL and HADMPL. These cover the first two objectives. The fifth research question is answered by the third objective, which introduces a binary and multi-objective version of the BAT algorithm for feature selection (MOBBAT). Finally, the last research question is covered by the fourth objective. This objective combines the EBAT-MLP algorithm with the best features selected by MOBBAT to produce a single and new intrusion detection approach, called MOB-EBATMLP.

Table 1.1: Mapping of research questions to objectives and contributions in this thesis

Chapter	Research Question	Research Objective	Contribution
4	-What metaheuristic algorithm(s) can be used to train neural networks for the purpose of intrusion detection? -Does hybridization of metaheuristic algorithms produce better algorithms with high balance between exploration and exploitation processes?	-To design and develop a metaheuristic technique that can be used to improve the performance of training neural networks for the purpose of IDS. The developed technique is to show better convergence and fitness accuracy for solving single and constrained-objective optimization problems.	-Enhance Bat algorithm: **Propose** a new EBAT algorithm. -Hybridize ABC & MBO algorithms: **Propose** a new HAM algorithm. -Hybridize ABC & DA algorithms: **Propose** a new HAD algorithm.
5	-How to improve the training of neural network models such that the learning algorithm can converge fast without trapping in local minima? -Can metaheuristic algorithms be used for training neural networks to produce the desired high accuracy over traditional algorithms?	-To adapt the developed metaheuristic algorithm for the supervised training of Multi-Layer Perceptrons (MLPs). The proposed training method would incorporate suitable data representation and suitable fitness measure for classification applications.	A method for adapting the new metaheuristic algorithms to train MLP: **Propose** three IDS models: 1. **HAMMLP** 2. **HADMLP** 3. **EBATMLP**
6	-How to combine a single-objective metaheuristic technique for training neural networks and a multi-objective metaheuristic for feature selection in a unified model of intrusion detection with the promised improved detection accuracy and reduced false alarm rate?	-To propose a binary, multi-objective version of any suitable metaheuristic algorithm, for feature selection, based on the wrapper approach. The proposed algorithm aims to minimize the number of features, thereby improving the task of their classification. -To design and implement the final new intrusion detection approach that utilizes the capabilities of MOBBAT algorithm to selects the optimal features from network packets as a first stage. The second stage passes these features to EBATMLP model for the detection of intrusions.	-Develop a new algorithm, namely, Multi-Objective Binary Bat Algorithm (**MOBBAT**). - Develop the complete new approach for intrusion detection, which is called (**MOB-EBATMLP**).

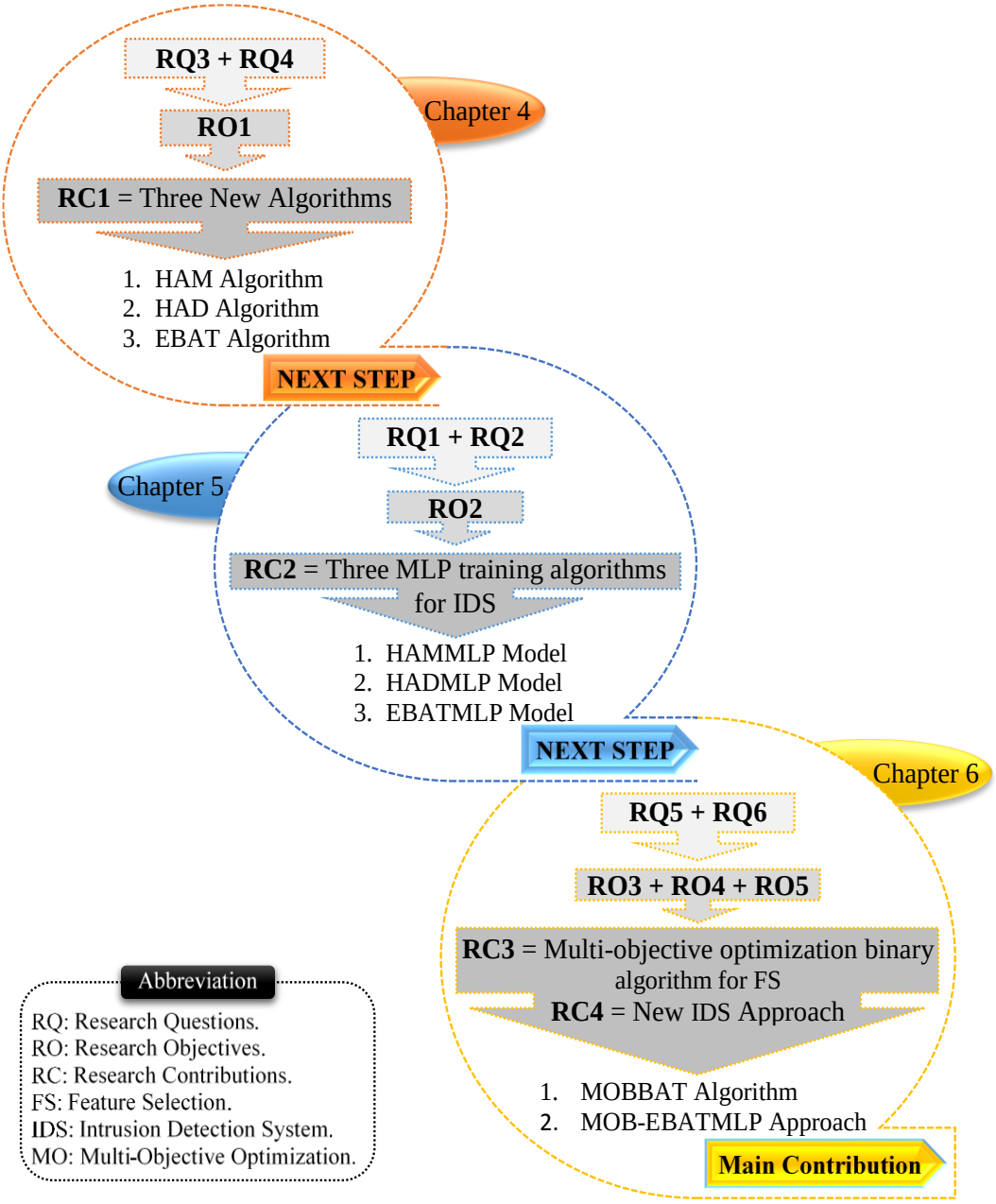

Figure 1.3: A Summary mapping between RQs, ROs, and RCs of this research

1.6 Research Scope

This study focuses on the accuracy of detecting anomalous activities in a computer network caused by intruders, whether they are originating from outside the network (Network-based intrusion detection),or from inside the network (host-based intrusion detection), including what is so-called hybrid intrusion detection (Akhyari and Fahmy, 2014; Chowdhary et al., 2014).

This research relies on the use of algorithms from the field of swarm intelligence and artificial neural networks, which are amongst the most important and popular techniques in the realm of computational intelligence, to fulfill the objectives of the thesis. Figure 1.4 illustrates the scope of this thesis, showing the used concepts and their relationships.

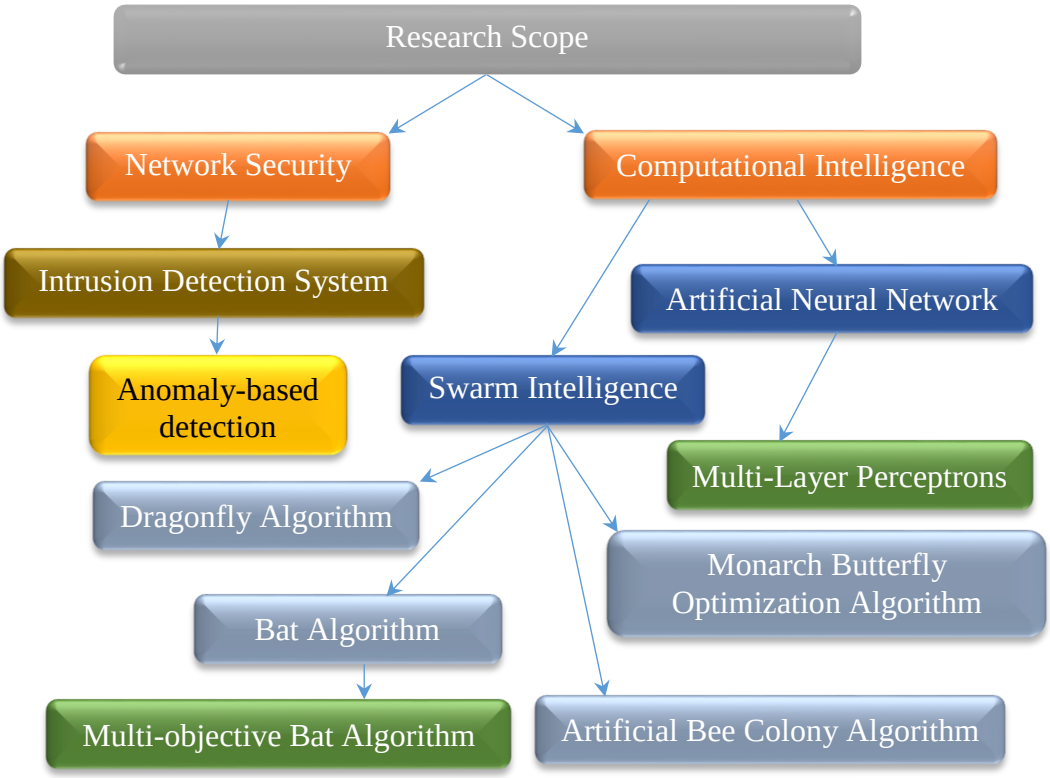

Figure 1.4: Scope of Research

1.7 Research Contribution

The main solution introduced in this research is a new approach for intrusion detection system, based on the famous concept of computational intelligence (CI). Computational intelligence is an umbrella for many concepts and algorithms, among which the most popular are swarm intelligence (SI) and Artificial Neural Networks (ANN) (Ahmad, 2014; Amudha and Rauf, 2012; Iftikhar and Fraz, 2013; Kolias et al., 2011; Revathi and Malathi, 2013). This research seeks to solve the problem of

increasing detection accuracy, and reducing the false alarm rate of intrusion detection systems, by improving the classification process and the selection of features (Hasani et al., 2014; Othman et al., 2013; Rufai et al., 2014). The achieved contributions of this research can be summarized in the following points:

1. Three new metaheuristic algorithms. The first algorithm, Enhanced Bat Algorithm (EBAT) is derived from the classic BAT algorithm, while the other two algorithms (Hybrid Artificial Bee Colony/Monarch Butterfly, HAM, and Hybrid Artificial Bee Colony/Dragonfly Algorithm, HAD) result from hybridizing the artificial bee colony optimization with the monarch butterfly algorithm and with the dragonfly algorithm, respectively. Theses hybrid algorithms employ the exploitation and exploration capabilities of both composite algorithms to optimize the search for local and global optimal solutions.

2. A method for adapting the new metaheuristic algorithms above for the training of Multi-Layer Perceptrons. The resulting training metaheuristic algorithms attempt to reach optimal weights and bias values for the MLP, which in turn leads to high classification performance.

3. The design and implementation of a two-phase system to improve the detection rate and reduce the false alarm rate of intrusion detection. The first phase uses the developed algorithm of an efficient feature selection based on binary and multi-objective BAT algorithm for wrapper-approach based feature selection, is called (MOBBAT), This algorithm is based on the weighted aggregation approach, uses a new fitness function to (minimize the number of features, minimize the classification error rate and minimize the false positive rate) in

order to improve the performance of IDS. The training of the classification algorithm. The second phase uses the features received from the first phase to classify the traffic based on the EBAT algorithm for MLP Neural Networks (EBAT-MLP), the new approach is called the (MOB-EBATMLP).

1.8 Research Methodology

The methodology of this research is divided into four main stages that aim to achieve the objectives of the research, as shown in figure 1.5. As shown in the diagram, the followed steps include: (1) reviewing related literature to identify and analyze existing studies, and then define the research problem, (2) the design of the two main components of the proposed approach, which include the feature selection technique and the metaheuristic algorithm for training the neural network, (3) the implementation of the proposed approach, integrating the two previous components in a coherent system, and (4) the evaluation of the new approach and assessment of the result by comparing it with other approaches.

In the first phase, the research problem is identified and the literature related to the research is reviewed. This phase formulates exactly the research problem and performs a comprehensive analysis of existing studies on the problem of research.

In the second phase, the solution for the research problem is designed and developed. The steps in this phase reflect clearly and directly on the objectives of the research, and accomplish the core of the objectives. As shown in figure 1.5, this phase consists of three major elements. The first element is the design of three new meta-heuristic algorithms, EBAT, HAM and HAD, to help overcome the shortcomings of the traditional metaheuristic algorithms. The second element is the training of the neural network by the new algorithms. The aim here is to get rid of the imperfections

in traditional training algorithms, reducing the computational complexity and the problems of tripping in local minima, as well as the slow convergence rate of current learning algorithms.

The last element of this phase is the selection of the important features from each network packet, achieved by the EBAT-based optimization as the wrapper classifier for the feature selector. This optimization relies on using a binary and multi-objective variation of the bat algorithm. The output of this step is an optimal subset of the features, which will be sent to the EBAT-MLP algorithm. These enhancements would lead in turn to enhance the ability to detect intrusion packets, which is the main objective of this research.

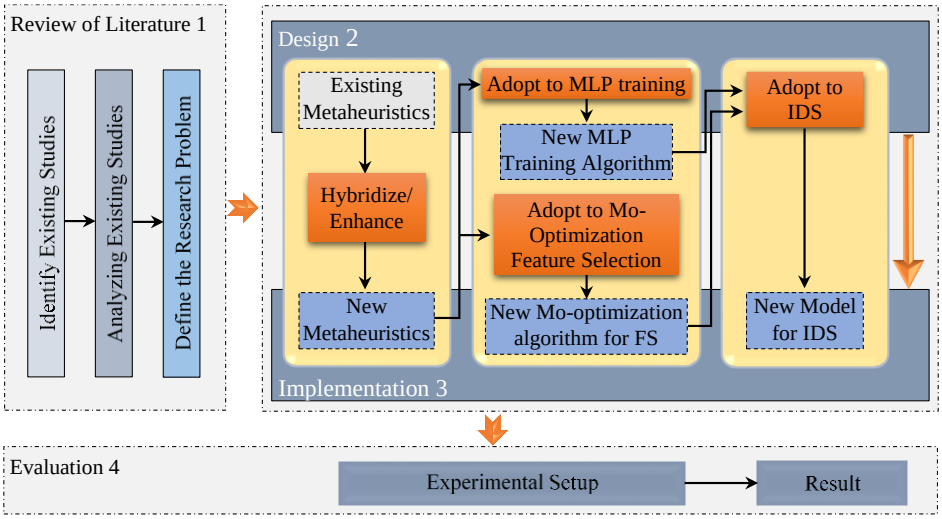

Figure 1.5: Research Methodology

In the third phase, the research design is implemented, and both the optimized selected features and the optimized training of neural networks are integrated into a coherent system to classify network traffic. Finally, the proposed approached is tested and evaluated in the fourth phase, based on its effectiveness in increasing detection accuracy and decreasing the false alarm rate. To evaluate the performance of detection in the new approach, this phase uses four of the most popular benchmark datasets:

KDD CUP 1999, NLS-KDD, ISCX2012 and UNSW NB15, which are frequently used by the research community to evaluate intrusion detection systems.

1.9 Thesis Outline

This thesis is divided into seven chapters, a references section and an appendices section. The contents of each chapter are as follows.

Chapter One introduces the problem statement of the thesis, specifies the scope of the research, the objectives expected from it, its contributions, the general methodology of the work, and finally summarizes the organization of the thesis.

Chapter Two offers the literature review. It guides the reader to the algorithms, techniques and the resources of the research domain, especially those related to the components of this work. In particular, it provides the reader with a background on the concepts of intrusion detection, artificial neural networks, artificial bee colony, dragonfly algorithm, bat algorithm, monarch butterfly algorithm, multi-objective optimization and the corresponding related work in the literature as well as the approaches that are proven effective in the field.

Chapter Three presents the flow of the research methodology in this thesis by introducing the components and the relationship between them in order to clarify how the proposed solution is designed. It explains the proposed approach and the involved algorithms at all stages, followed by the characteristics of the employed datasets and benchmarking functions.

Chapter Four introduces three new metaheuristic optimisation algorithms. This chapter also presents the evaluation of the proposed algorithms' performance using 13 benchmark test functions and statistical analysis.

Chapter Five introduces the technique for adapting the optimization algorithms developed in Chapter 4 for the training of MLPs. The performances of the proposed methods, called EBATMLP, HAMMLP and HADMLP, respectively, are verified using four benchmarking datasets. Similar to the previous chapter, the proposed training techniques are validated against performance metric supported by statistical analysis.

Chapter Six introduces the intrusion detection approach that uses a multi-objective version of the Bat algorithm for feature selection, based on the wrapper approach. The proposed algorithm is named MOBBAT. This algorithm forms the first stage of the intrusion detection approach to select the appropriate features from network packets. EBATMLP is then used for the classification task. The whole system is implemented using MATLAB. This chapter covers in depth the conducted experiments to evaluate the implemented approach as well as the obtained results, including the discussion of the results.

Chapter Seven concludes the thesis with a short summary of the work, and concise comments on the findings, besides a brief discussion of the direction to go from here.

Each chapter except the first and last begins with an introduction and concludes with a summary.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter provides the reader with the necessary background on the main concepts and components that have been used throughout this work, and the previous works based on these components. Figure 2.1 shows the fundamental concepts and components that would be covered by this chapter. The chapter starts by giving a brief background on network intrusion detection systems, followed by the basic concepts of artificial neural networks, feature selection, multi-objective optimization technique, and swarm intelligence, all of which constitute an essential part of the proposed framework in this thesis. Next, the application of swarm intelligence methods to optimize both feature selection and the training on neural networks is discussed in terms of previous works, to put the work of this research in perspective.

2.2 Intrusion Detection Systems

An intrusion detection is defined by (Balasubramaniyan et al., 1998; Mukherjee et al., 1994; Snapp et al., 2017) as: ”the problem of identifying individuals [or threat agents] that are using a computer system without authorization i.e. crackers and those who have legitimate access to the system but are exceeding their privileges i.e. insider threat”.

Generally, intrusion detection methodologies are classified into three basic categories: signature-based detection, anomaly-based detection and hybrid detection. These three methods perform the essential function of monitoring the events that occur in a computer system or network, analyzing the events, detecting suspicious events

(intrusions) and raising an alarm when discovering the intrusion. The fundamental difference between them lies in the events analysis method, where each one has different approach from the other. In the following section will be discussed these methods with more details.

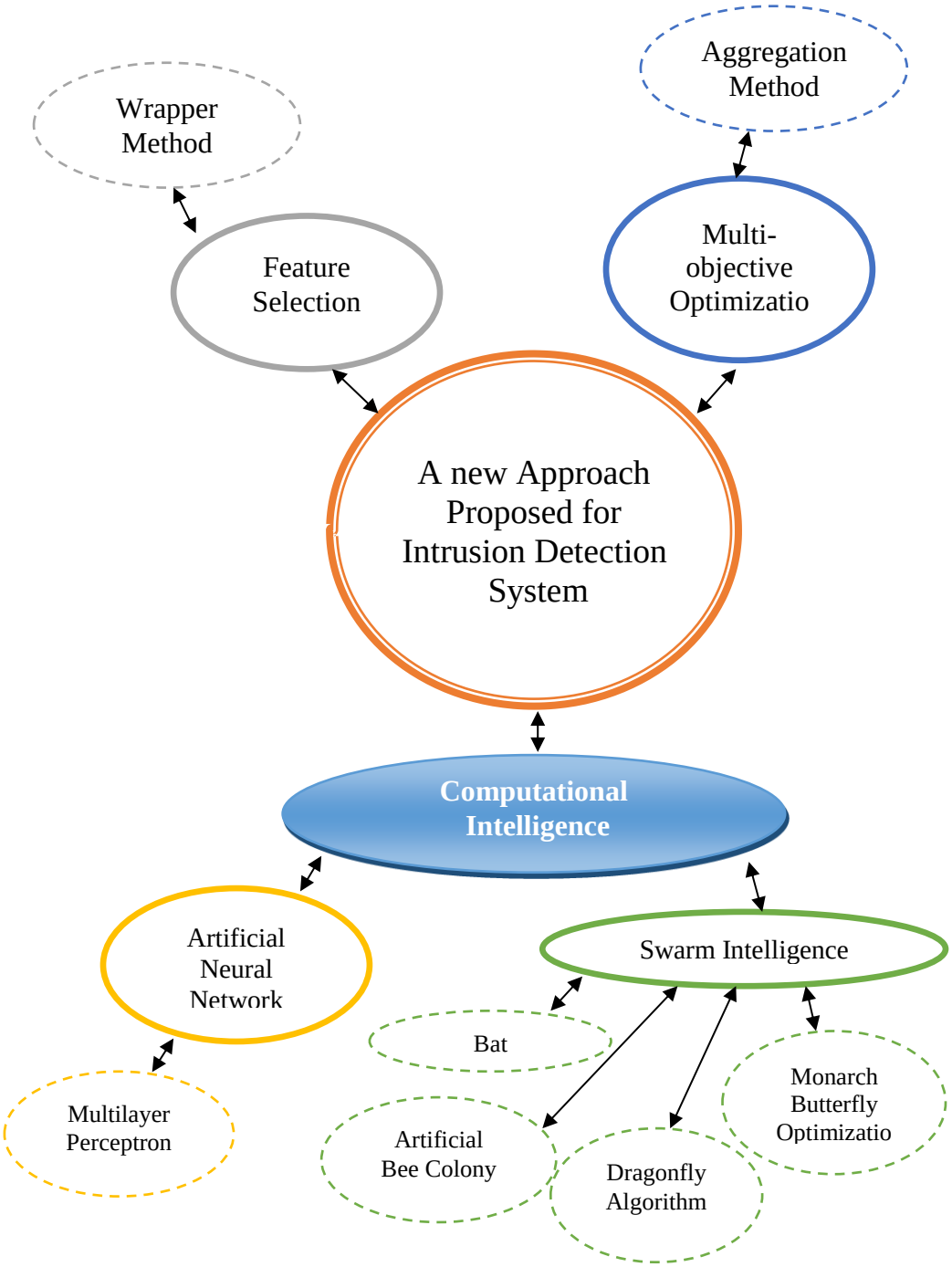

Figure 2.1: The related work and literature survey

2.2.1 Anomaly-Based Detection Method

An anomaly based detection method is sometimes called as behavior-based detection, as it is based on monitoring the behavior of the network. Anomaly is a deviation from the usual or normal activities to unusual activities, and these activities are measured by profiles that represent expected behaviors derived from monitoring regular activities of the host, users, and the network connections over a period of time (García-Teodoro et al., 2009; Liao et al., 2013; Zhang and Shen, 2004).

According to (Scarfone and Mell, 2007; Wu and Banzhaf, 2010) the anomaly based detection has a main advantage that distinguishes it from the rest of methods, which is the high potential and effectiveness of detecting previously unknown threats (new intrusions without previous knowledge). However, this method creates a base profile depending only on the normal data; therefore, any deviation from the profile is considered as an anomaly, which might introduce false positives.

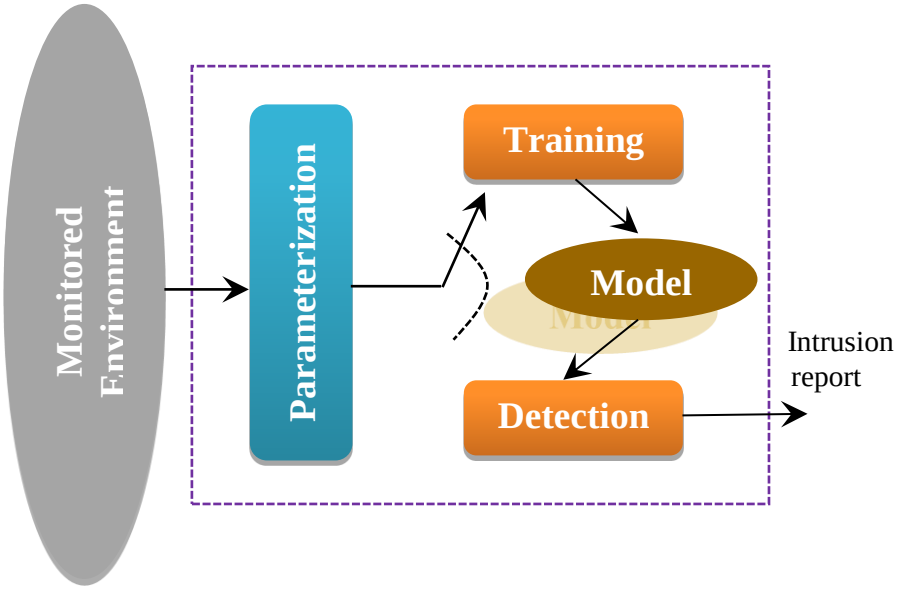

Figure 2.2: Generic A-NIDS functional architecture (García-Teodoro et al., 2009)

Despite the many different approaches of anomaly IDSs, they all share the three stages of Parameterization, Training stage and Detection (Estevez-Tapiador et al.,

2004; García-Teodoro et al., 2009). Figure 2.2 shows these three basic stages. Parameterization is the stage where the IDS interacts with the external environment and the monitored cases of the target system are represented in a pre-established model. The training stage is used to create a profile of the normal behavior of the system. Finally, the detection stage uses the profile that was created in the training stage and compares it with the current (parameterized) observed traffic of the system. If the model detects any deviation from the normal behavior, then an alarm is raised.

2.2.2 Signature-Based Detection Method

Signature-based detection is also called knowledge-based detection or misuse detection. The method is based primarily on the possession of prior knowledge about the threats and attacks, called *signatures*. The signatures represent either patterns or strings that are compatible with a known attack or threat (Liao et al., 2013). The signature detection is based on comparing a pattern or string, which is defined and stored beforehand, against captured events in order to identify possible intrusions.

In other words, the signature detection use the accumulated knowledge to detect the known attack or threat, but most signature detections fail to detect unknown attacks or threats, because it's based on only known attack patterns (signatures) and it is difficult to detect malformed or new signatures (Cathey et al., 2003).

2.2.3 Hybrid Detection Method

Hybrid detection method is based on the integration between anomaly intrusion detection and signature intrusion detection. The main advantage of the hybrid method is its ability to overcome the weaknesses of signature and anomaly detection (Kim, H. J. et al., 2007; Xu and Luo, 2007). In general, this type of detection has the capability

to achieve high detection accuracy and low false alarms by virtue of the signature detector component, and is capable of detecting new attacks by virtue of the anomaly detector component (Zhang and Zulkernine, 2006).

2.2.4 Intrusion Detection Technology Types

An intrusion detection technology can be categorized into two types which is based on the way in which they are deployed to inspect suspicious activities and what event types they can recognize (Modi et al., 2013; Mukherjee et al., 1994; Sabahi and Movaghar, 2008; Stavroulakis and Stamp, 2010): Host-Based Intrusion Detection System (HIDS) and Network Based Intrusion Detection System (NIDS). The fundamental difference between them is that, in general, the main task of the NIDS technology is to protect the entire network, on the other hand the HIDS responsibility is to protect the critical endpoints, so there is no need to analyze the traffic across the network like NIDS.

2.2.4(a) Host-based intrusion detection system (HIDS)

The responsibility of host-based detection systems lie in monitoring resources only on the host machines, such as applications and system log files which are used to collecting all events, and then analyze records of events in order to recognize if there is an intrusion or not. Figure 2.3 illustrates the location of HIDS on the network. HIDS are most often positioned on critical hosts such as servers containing sensitive information and publicly accessible servers (Liao et al., 2013; Scarfone and Mell, 2007).

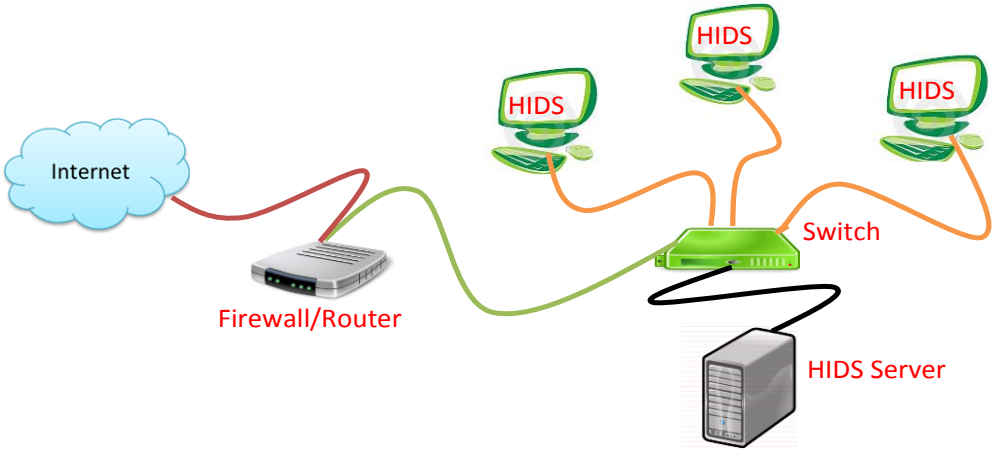

Figure 2.3: Host based intrusion detection system

2.2.4(b) Network-based intrusion detection system (NIDS)

Network-based intrusion detection systems monitor network traffic among all hosts/users, through an external interface like a detection sensor (sniffer) that is placed at a hub or switch to capture all packets traveling through network segments. The NIDS could be either a device and/or program that monitors data traveling across a network at specific network segments and analyzes the activities of the network and applications and protocols, in order to decide whether these activities are normal or abnormal (Liao et al., 2013; Scarfone and Mell, 2007). The major advantage of NIDS is that a single engine can be used to monitor the complete network or segments of it, without the need to installing custom software on each users/hosts like the HIDS, as shown in figure 2.4. It usually also has highest ability and faster response. Furthermore, intrusions can attack directly the HIDS and its lower-level services, but it is difficult to attack the engine of NIDS directly.

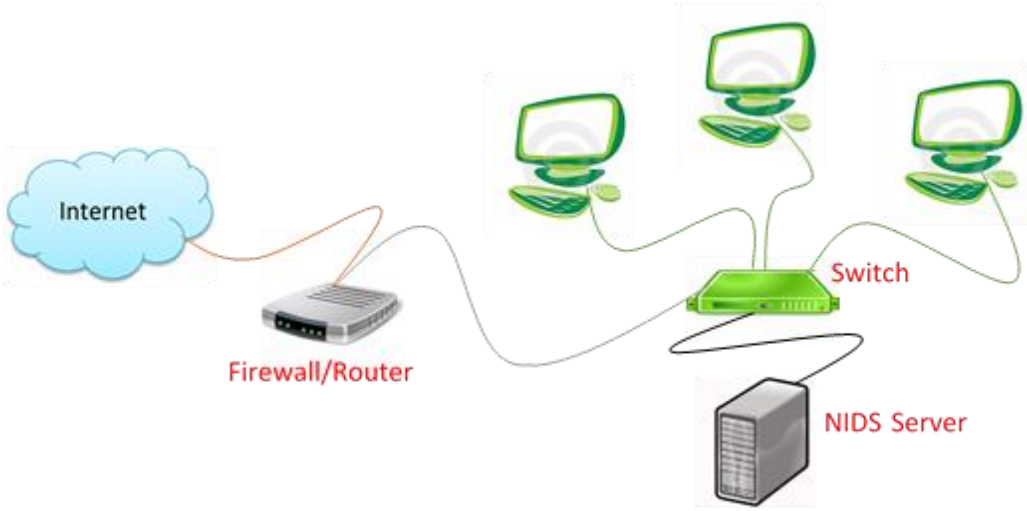

Figure 2.4: Network based intrusion detection system

2.3 Artificial Neural Network (ANN)

Artificial neural networks are one of the most important techniques in the computational intelligence. It has the ability to simulate the human brain, learn, memorize and still generalize. Furthermore, the scope of its use is very wide in a variety of fields in science and industry. It has the ability to perform linear, non-linear and parallel modeling (Alavala, 2008; Tang et al., 2007; Zilouchian, 2001) to achieve such tasks as pattern recognition and time series prediction.

First appearance of ANNs was in the 1950's which was driven by the attempt both to comprehend the human brain in addition to simulate its strength. The basic building block in the biological neural system is called the *biological neuron*. Artificial neural networks, on the other hand, are based on a basic unit called *artificial neuron*. Figure 2.5 shows the difference between the two systems. The main difference lies in the input signal. Whereas the biological neural system can only receive input signal as discrete electrical pulses (discrete variable), the artificial neural network can receive input signal as continuous as well as discrete variables (Langley & Laird, 2006).

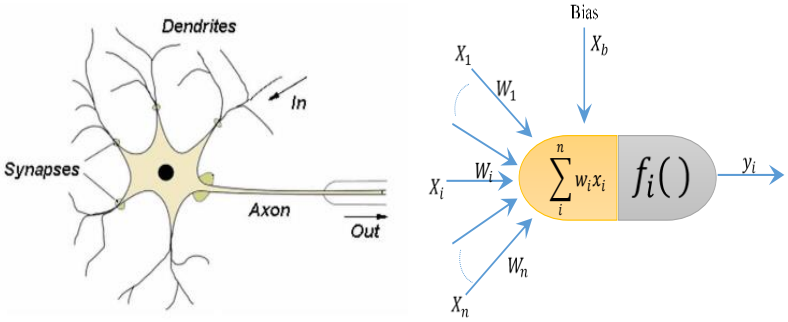

Figure 2.5: Biological neural system vs. artificial neural network

Several models for neural networks have been suggested, it is possible to say that one model is better than others by the high efficiency in the performance of the learning algorithm used in the model. Learning algorithm is a method that helps in calculating the error rate while training the network on a given task, and then adjusting the parameters of the model to memorize the training. The architecture or topology of the neural network refers to the method by which the neurons are connected with each other. The neurons are organized in layers, where each layer contains a set of specific and non-interconnected neurons. All neurons in the first layer connect with all the nodes in the layer that followed.

There are different varieties of ANN models, which can be classified based on the type of feeding and the number of layers. The category of an ANN according to feeding is divided into two types: feed-forward and feed-back. Based on the number of layers there are two types: single layer and multi-layer neural networks. The Feed Forward Neural Network (FFNN) is popular as a special or a stranded class of multilayer neural networks, also called Multiple-Layer Perceptron (MLP) networks. Figure 2.6 illustrates a standard feed-forward neural network. The network in the figure consists of three layers, namely an input layer, a hidden layer and an output layer, each layer containing three neurons. In some research articles on neural