Intelligent Hybrid Approach for Classification Accuracy of Intrusion Detection System

Prepared By:

Mustafa Nihad Abbas

Supervisor

Prof.Dr.Mohammad Ahmad Alfayoumi

This Thesis Submitted in Partial Fulfilment of the Requirements for

The Master Degree in Software Engineering

Isra University

Amman, Jordan

2019/2020

AUTHORIZATION STATEMENT

I am Mustafa Nihad Abbas, authorize Isra University to provide hard copies or soft copies of my thesis to libraries, institution or individuals upon their request.

Name: Mustafa Nihad Abbas

Signature: 

Date: 17/12/2019

اقرار تفويض

اني مصطفى نهاد عباس، افوض جامعة الإسراء للدراسات العليا بتزويد نسخ من رسالتي ورقياً و إلكترونياً للمكتبات او المنظمات او الهيئات و المؤسسات المعنية بالأبحاث و الدراسات العليا عند طلبها.

الإسم: مصطفى نهاد عباس

التوقيع:

التاريخ: ١٧/١٢/٢٠١٩

The undersigned have examined the thesis entitled (**Intelligent Hybrid Approach for Classification Accuracy of Intrusion Detection System**) presented by (**Mustafa Nihad Abbas**) a candidate for the degree of Master of information technology in software engineering and hereby certify that it is worthy of acceptance.

17/12/2019	
Date	**Prof.Dr.Mohammad Ahmad Alfayoumi**
15.12.2019	
Date	**Dr. Mudhafar Al Jarrah**
16.12.2019	
Date	**Dr. Venus W. Samawi**

LIST OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

IDS	Intrusion Detection System
DDOS	
R2L	
GA	Genetic Algorithm
GWO	Grey Wolf Optimizer
PSO	Particle Swarm Optimization
FFA	Firefly Algorithm
ACO	Ant Colony Optimization
NFL	No-Free Lunch Theorem
GD	Gradient Decent
KNN	K Nearest
SVM	Support Vector Machine
NSL	Network Socket Layer
BP	Backpropagation
PCA	Principle Components Analysis
RF	Random Forrest
SOM	Self-Organization Maps
SFLA	Shuffled Frog Leaping Algorithm
BBO	Biogeography-Based Optimization
PSO	Particle Swarm Optimization
ABC	Artificial Bee Colony
CS	Cuckoo Search
BA	Bat Algorithm

ABSTRACT

Intrusion detection system (I.D.S) is an essential component, which enhances the security of computer systems by actively detecting all forms of attack at the early stages. The main use of IDS is the monitoring of the network traffics and analyzing the behavior of the users in searching for any abnormal activity or attack signature for real-time intrusion detection. The main weakness in any IDS is their inability to offer adequate sensitivity and accuracy; coupled with their inability to process enormous data. To address these issues (such as the increasing traffic, huge behavior profiles, large signature databases, and the inability of differentiating normal behaviors from the suspicious ones), several algorithms have been developed. Hence, the main aim of this work is to choose the differentiating features for the development of an optimal machine learning algorithm which can offer high detection rates, fast training, and testing processes offline. The proposed machine learning model contains a feature selection algorithm (wrapper type) which is based on the integration of the Binary Firefly algorithm enhanced for feature selection by crossover operator taking from the genetic algorithm, called (GA-FA) with the Naïve Bayesian Classifier (NBC). The performance of the proposed model was tested on NSL_KDD data sets prepared by the MIT Lincoln Laboratory. The model testing was based on several experiments and different scenarios (the effect of swarm size, number of iterations, and the $Swap$). For evaluating the ability to select the minimum number of features with the higher value of classification accuracy, the algorithm worked perfectly and selected a comparable number of features. The model achieved the best average accuracy of 97.011%. In conclusion, the proposed feature selection algorithm has the ability to select the most relevant features which enhance the classification accuracy of the network intrusion detection system.