An Intrusion Detection System Based on Hybrid of Particle Swarm Optimization (PSO) and Magnetic Optimization Algorithm (MOA)

Siti Norwahidayah Wahab, Noor Suhana Sulaiman,
Noraniah Abdul Aziz, Nur Liyana Zakaria,
Nurul Farahah Abdul Halim and Ainal Amirah Abdul Aziz

April 18, 2021

An Intrusion Detection System Based on Hybrid of Particle Swarm Optimization (PSO) and Magnetic Optimization Algorithm (MOA)

Siti Norwahidayah Wahab[1] Noor Suhana Sulaiman[1] Noraniah Abdul Aziz[1] Nur Liyana Zakaria[1] Ainal Amirah Abd Aziz[1]

[1] Faculty of Computer, Media and Technology Management, University College TATI,
Terengganu, MALAYSIA
norwahidayah@uctati.edu.my

IDS (Intrusion Detection System) is a security component that protects computer and network systems. Variety of methods have been developed to improve the IDS accuracy. One of the most recent approaches is the use of real-time monitoring and irregular activity detection. When an intrusion is detected, a message will be sent to the network administrator. One of the disadvantages of IDS is the possibility of a bad packet by-passing through network traffic. As a result, an improvement on the Artificial Neural Network (ANN) is explored in this study to enhance attack detection in IDS. Standard and attack events are described using the NSL-KDD dataset. In this study, the Magnetic Optimization Algorithm (MOA) is combined with Particle Swarm Optimization (PSO) named PSOMOA, thus to increase the classification rate and achieve high detection accuracy in IDS. MOA is a heuristic optimization algorithm which deals with attraction between particles scattered in the search space and inspired by magnetic field theory in physics. NSL-KDD dataset represented as attacks and normal activities used in this study. Smurf and Neptune attacks are selected for testifying detection and classification ability of attack category of proposed PSOMOA. During the experimentation process, four of the most important features of the dataset were selected. The PSOMOA findings are compared to those of the other form, which employs PSO and MOA. According to the obtained results, the proposed PSOMOA could increase IDS accuracy by up to 99.5 percent.

Keywords: Artificial Neural Network, Magnetic Optimization Algorithm, Particle Swarm Optimization, Intrusion Detection System, NSL-KDD.

1 Introduction

Intrusion Detection System (IDS) protects the network from malicious activity. An intrusion detection system may also be thought of as "powerful security elements capable of detecting, preventing, and responding to computer attacks." [1]. Recent technology has been used to track and identify abnormal behavior in real time. When an intrusion is observed, the IDS notifies and sends alerts to the network administrator. Until now, IDS was used throughout the network to detect an intrusion by monitoring network traffic. Intrusion detection has previously relied on evaluating network flows, logs, and device events [2]. Deploying an IDS in a large-scale network, on the other hand, is a challenging task since it exposes the network to a range of attacks. The problems and drawbacks of IDS do not justify a business or company's refusal to use it. This research has emphasized the importance of studying and improving the best way to solve those issues.

Many analysts nowadays use a modern methodology to address IDS's nagging issues. Artificial Intelligence (AI) is the study of the possibility of creating intelligent systems that can reason and think like humans. IDS employs a variety of AI techniques. The Artificial Neural Network (ANN) can solve classification and regression problems. Its ability to learn from observing the dataset, however, has some limitations. On the other learning methods, Feedforward Neural Network (FNN), aim to find the best combination of connection weight and biases to achieve the lowest possible error. FNN frequently converge to points that are the best local solution but not globally suitable for large network. Simulated Annealing (SA), Genetic Algorithm, and other heuristic optimization methods for FNN have been suggested by several researchers. Genetic algorithm (GA), Particle Swarm Optimization (PSO), Magnetic Optimization Algorithm (MOA), and Differential Evaluation (DE) are number of examples of optimization algorithms [4]. According to Mirjalili [4], it has some disadvantages over other optimization approaches, such as slow convergence speeds.

Denial of Service (DoS) attacks degrade server output by flooding ICMP traffic, and they have been happening since February 2000 [5]. Aside from that, DoS will cause a victim's server memory resources to become full by repeated sending TCP packet for requesting to start a TCP session [5]. Smurf attack and Neptune attack, both are kind of DoS attacks. As such, detecting DoS attacks is an essential and required tool and technique to employ, particularly on Smurf and Neptune attack. As a result, a combination of Particle Swarm Optimization (PSO) and Magnetic Optimization Algorithm (MOA) called hybrid PSOMOA was proposed to solve the ANN drawbacks.

2 Literature Review

In network analysis, network datasets are often used. Large amounts of time are spent processing and transmitting data, as well as a higher rate of false alarms in attack detection, all of which result in harm and unsafe conditions for online users, such prescribed in IDS dataset [6].

Researchers have suggested several optimization strategies to achieve high precision in intrusion detection [3]. Previous work and methods will be highlighted in this topic, such as the hierarchical clustering algorithm [7], removal feature selection and support vector machine [8], gravitational search algorithm [3], and pattern recognition (Ernesto et al, 2015).

Horng [7] proposed a combination of hierarchical clustering and support vector machine (SVM), in which the author used the (Balanced Iterative Reducing and Clustering using Hierarchies) Birch algorithm to reduce the KDD CUP 1999 dataset. Before dataset training, the SVM, an algorithm created a reduced and high-quality dataset from the original KDD CUP 1999 dataset. The Birch algorithm is an unsupervised data mining algorithm for performing hierarchical gathering over large datasets [7]. The experimentation resulted in a high accuracy of 95.72 percent and a low false positive rate of 0.7 percent using the proposed techniques.

The other method is Gradual Feature Removal (GFR) [8]. The paper uses 19 important features to represent a network visit [8]. To achieve better results, the author also used a hybrid feature selection approach that combines wrapper and filter methods. The first stage is data pre-processing, which involves creating a raw database and removing duplicate data. The dataset was then trained using the Artificial Neural Network (ANN) process, which classified the data using 41 KDD CUP '99 features to find the best training sample with high accuracy. The final stage is feature reduction, which involves training and testing the dataset with 41 features and four separate feature reduction techniques before the author obtains 19 essential features using the GFR process.

Dastanpour [3] proposed the Gravitational Search Algorithm (GSA) to assist ANN in IDS. The GSA is a popular machine learning algorithm based on gravity law and mass interaction. The four conditions of mass, referred to as agents, are location, inertial mass, active and passive gravitational mass. The author divides the KDD CUP ’99 dataset into two phases which for testing and training. After that, the methods for reorganization established a structured format for datasets. When the ANN training is complete, the ANN classifies the testing dataset and outputs the accuracy of the device detection as a result. Following the acknowledgment of the ANN end, the GSA optimizes the ANN. The outcome of ANN (without the GSA) will be compared to the result of ANN with the GSA (with GSA). For the dataset, author decide to set 1 represent for the attack and 0 as normal for separate the attack and normal one. The experimental result show that the ANN with GSA contributes high accuracy (98.7%) rate of detection. Proposed method capable to optimize and improve the ANN performance. Besides, the method also achieves 1.0 accuracy with only 39 critical features of KDD CUP ’99 [3].

Tian and Liu [9] proposed a procedure that uses an ANN and a PSO algorithm (PSOA). PSOA was proposed by the authors because it can address the problem of searching performance. The paper used a rough collection of ANN data to select a subset of input attributes and used PSOA to improve ANN efficiency. The authors used an equation to determine each fitness particles, update velocity and position, and update local best and global best particle to integrate the PSOA [9].

Eight rough set features were chosen, with six nodes in the ANN output layer. One of the five output nodes was used for standard, while the other four were used for attacks. The training set is 80% and testing set is 20% where the total of the data is 460. The proposed method has a higher level of stability and can detect more attacks with a lower mean square error. The PSOA, on the other hand, has some flaws, including a slow convergence rate [4].

3 NSL-KDD Dataset

NSL-KDD dataset is offline network data based on KDD 99 dataset where it contains 41 attributes and one class attribute. NSL-KDD is a data set suggested to solve some of the inherent problems of the KDD'99 data set where it eliminates noise data in KDD'99 data set. The NSL-KDD dataset is smaller than the KDD99 dataset which has duplicate records. The advantages of NSL-KDD data set are:

(i) The train collection does not contain any duplicate records, so the classifiers would not favor more frequent records.
(ii) Since the proposed test sets contain no duplicate records, methods with higher detection rates on frequent records have no impact on the learners' performance.
(iii) The number of records selected from each difficulty level group is inversely proportional to the percentage of records in the original KDD data collection.
(iv) As a result, different machine learning methods' classification rates vary more widely, making an accurate evaluation of different learning techniques more reliable.
(v) Since the train and test sets contain a reasonable number of records, it is more practical to test the entire set rather than a small subset at random.

NSL-KDD dataset divided into two sets which are training sets and testing sets. Each record of the dataset is continuous, discrete and symbolic forms. Protocol_type feature that used in this study represent 2 as tcp, 3 as udp, 4 as icmp and 5 as other symbols. Besides, for the result used 0 for Normal and 1 as Attack. The attacks can be categorized as follows:

(i) Denial of Service Attack (DoS): DoS attack is an aggressive attack that an attacker sends many ping packet to make the network flooded with packet and become congested. Such that, the attacker can denies the legitimate user access to the servers (Mahbod et al., 2009).
(ii) User to Root Attack (U2R): The attacker has a local access to the victim machine and to gain the root access to the system [11].
(iii) Remote to Local Attack (R2L): The attacker did not have a local access to the victim machine but tries to gain the local access as a user to the machine [11].
(iv) Probe Attack: Intruders try to grab information about the target machine and aim to bypass the security controls (Mahbod et al., 2009). Generally, most researchers used NSL-KDD which include the total of dataset is 494,020. The distribution dataset for Normal is 97280, Probe is 4107, DoS is 391458, U2R is 52, R2L is 1124 [12].

4 Methodology

The methodology for this research is mainly divided into five sections; in which the first part will be on collecting and processing dataset to be used for training ANN in IDS. The second part will focus on applying the hybrid PSOMOA on dataset. The dataset will then also be used to classify the normal and abnormal activities. The output value of PSOMOA will support ANN to maximize the classification rate. The final parts involved the analysis and comparison of the optimization by using ANN supported by PSOMOA.

4.1 Pre-Processing

There are 41 attributes and one class attribute in the NSL-KDD data set. Some of the 41 attributes play no role in attack detection, whereas others play a minor role. The knowledge gain attribute evaluation, gain ratio attribute evaluation, and correlation attribute evaluation algorithms are used by Bajaj et al. [10]. According to the researcher [10], attributes 9, 20, and 21 play no part, although attributes 15, 17, 19, 32, 40 have minimum role in detection of attack. An analysis of the NSL-KDD dataset reveals that features 7, 8, 11, and 14 have virtually all zero values. By eliminating these least available features from the dataset's training and testing sets, the dataset would be reduced to 29 features, resulting in a smaller dataset. Now that the dataset has been limited, it can be used for training and research. A total of 41 features were used in the training and testing, and feature reduction is not performed on dataset.

It is impossible to use all rows of dataset because it takes a lot of run time. Hence, in this study, only 4 critical dataset features selected and 200 rows input values will be used to train ANN. Besides, one column will be added for identifying each record as a result which are 0 for normal and 1 for attack in the standard format step. The reason of adding this additional row is to continue and understand the error reorganization in ANN. In order to make the dataset compatible, the given attributes are converted to a double data form with the ANN toolbox of MATLAB toolkit because it is only support the data in integer form [13]. The "protocol_type" feature converted with values like tcp is 2 and udp is 3. Not all protocol types selected because only 200 rows of dataset used to test the algorithm [13].

In this research, the MOA used to optimize the results of ANN. MOA makes the random agent calculate the mass value of each agent to optimize the ANN. The MOA parameters that used in this study is number of agents, maximum number of iteration, number of training samples, inertia weight, minimum weight, maximum weight and objective function.

4.2 Propose IDS Security System Based on Hybrid PSOMOA

The method proposed in this paper is for training ANN to optimize IDS with supported by the combination of PSO and MOA. First, this study tries to divide the dataset into two data section for training and testing. Then the methods try to develop the standard dataset format for the reorganization of ANN. After the training of the ANN is completed, the ANN will classify the NSL-KDD testing dataset and extract the accuracy output of the system detection, which will then be plotted and monitored it by the system. When the recognition phase of the ANN is completed, then the MOA data input will be the result of ANN. At this stage, the ANN reorganization will attempt to be optimized by MOA. Finally, after the results of the ANN are optimized by the MOA, they will by plotted to be compared with the ANN result (without MOA), such that the effects of MOA will be more understood in the ANN reorganization in the intrusion detection system using the dataset of NSL-KDD. The main idea and overall methods have been illustrated in Fig. 1. In order to support ANN in IDS optimization, the PSO will be implemented.

The training method involve once packet data is extracted. The useless data are removed. The knowledge is any keep as patterns to form a knowledge file. The information file contains immense patterns. The patterns square measure any processed to extract representative patterns which will be used for coaching the ANN with specific ANN rule. The result is a final weight matrix, which is saved in a large format. Incoming packets of data knowledge are stripped and any tangential information is filtered as part of the testing process. The data is then processed with the ultimate weights to produce a price in the ANN's output layer. The assisted performance is based on intrusion detection classification and testing is completed.

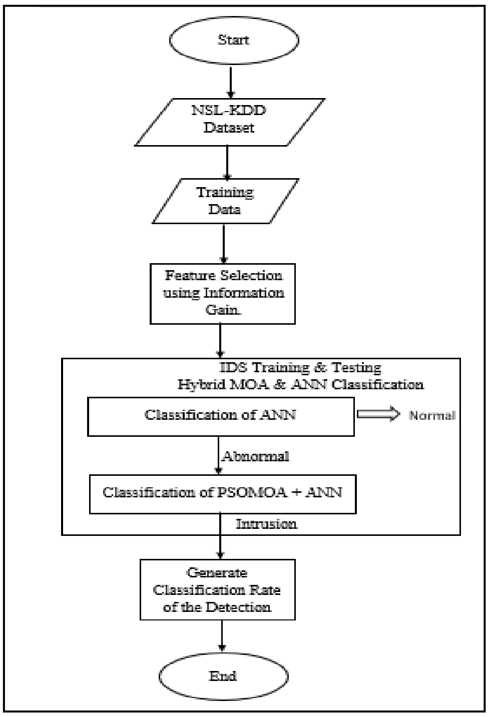

Start
NSL-KDD Dataset
Training Data
Feature Selection using Information Gain.
IDS Training & Testing Hybrid MOA & ANN Classification
Classification of ANN
Normal
Abnormal
Classification of PSOMOA + ANN
Intrusion
Generate Classification Rate of the Detection
End

Fig. 1. Process Flow

5 Result and Discussion

In this research, only 4 critical features selected to classify the attack and normal packet in IDS. The experimentation will compare the classification rate result with another best features selection. Another relevant features selected include 3, 5, 29 and 39 which 3 for Service (network service on the destination such as http, udp and etc), 5 for Source Bytes (number of data bytes from source to destination), 29 for Same Srv Rate (percentage of connection to the same service) and 39 for Dst Host Srv Serror Rate (Service error rate for the destination host) [14].

Besides, the other relevant dataset features is number 3, 23, 30 and 36 [15]. Feature 3 for Service (network service on the destination such as http, udp, etc), 23 is Count (number of connections to the same host as the current connection in the past two seconds), 30 for Diff Srv Rate (percentage of connections to the different services) and 36 for Dst Host Same Src Port Rate (same source port rate for destination host). The next relevant features from researcher [14] are 36, 37, 38 and 39 where 36 for Dst Host Same Src Port Rate (same source port rate for destination host), 37 is Dst Host Srv Diff Host Rate (Different host rate for destination host), 38 is Dst Host Serror Rate (error rate for destination host) and 39 is Dst Host Srv Serror Rate (service error rate for destination host).

The last relevant dataset features selected are 3, 6, 29 and 30 [14]. Feature 3 is Service (network service on the destination such as http, udp, etc), 6 is Dst Bytes (number of data bytes from destination to source), 29 is Same Srv Rate (percentage of connections to the same services) and 30 is Diff Srv Rate (percentage of connections to different services). In this study, all combination the dataset features will be simulated and produce up to total result of 37 different classification rate. Table 1 shows the relevant features of detecting the normal behavior, Smurf attack and Neptune attack.

Table 1. Relevant Features for Normal, Smurf Attack and Neptune Attack

Class Label	Relevant Features
Normal	3,6,12,23,25,26,29,30,33,34,35,36,37,38,39
Smurf	2,3,5,6,12,25,29,30,32,36,37,39
Neptune	3,4,5,23,26.29,30,31,32,34,36,37,38,39

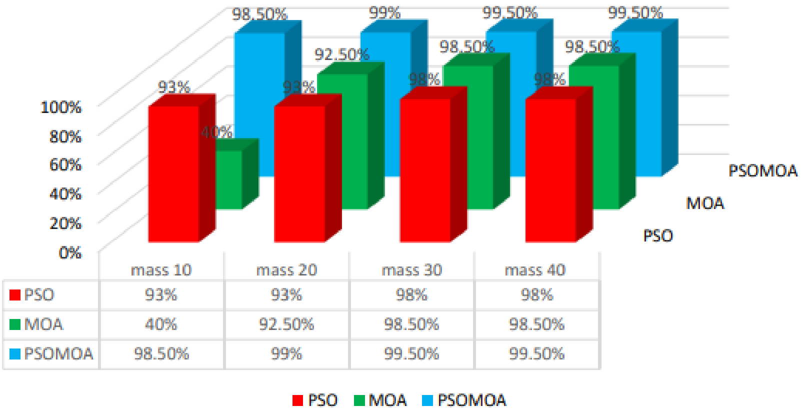
This study used most of the relevant features, to detect those attacks in IDS. Table 2 list the combination of relevant features to investigate to get the best features selection. The dataset will load in the MATLAB using the code of MOA, PSO and Hybrid of MOA and PSO to produce the high classification rate of the attack detection.

Table 2. Combination of relevant features of Normal, Smurf Attack and Neptune Attack

Class Label	Features	Features Name
Normal	2,3,4,5,6,12,23,	Protocol_type, Service, Flag, Src_bytes, Dst_bytes, Logged_in, Count, Serror_rate, Srv_serror_rate
Smurf	25,26,29,30,31, 32,33,34,35,36	Same_srv_rate, Diff_srv_rate Srv_diff_host_rateDst_host_count
Neptune	37,38,39	Dst_host_srv_count, Dst_host_same_srv_rate, Dst_host_diff_srv_rate, Dst_host_same_src_port_rate, Dst_host_srv_diff_host_rate, Dst_host_serror_rate, Dst_host_srv_serror_rate

In Fig. 2 shows, FNN using hybrid PSO and MOA (so called PSOMOA) is the better techniques for optimization on ANN that can achieve high accuracy compared with others. The parameter setting that suitable in this project is using masses 30, 500 for maximum number of iterations, 15 for hidden nodes, 200 training samples and 2 for inertia weight. Using this parameter setting with the optimization algorithm proposed, it can achieve high detection rate and high classification rate with low iteration numbers and masses. According to the result given, PSOMOA achieves the reliability because it reduces the probability of trapping in local minima.

PSOMOA's outcome demonstrates that it is capable of both searching and attracting people. In other words, the strengths of PSO and MOA have been successfully combined to produce excellent results in FNN preparation.



	mass 10	mass 20	mass 30	mass 40
🟥 PSO	93%	93%	98%	98%
🟩 MOA	40%	92.50%	98.50%	98.50%
🟦 PSOMOA	98.50%	99%	99.50%	99.50%

Fig. 2. Comparison of Masses 10, 20, 30 and 40 of MOA, PSO and PSOMOA

6 Conclusion

A new training optimization algorithm which are hybrid of ANN, PSO and MOA is introduced and investigated. NSL-KDD dataset used to represent a packet and simulated in the MATLAB toolkit. The project steps proposed as follows: collecting and processing dataset which select only 4 critical features for detection of two network attack categories to be used for training ANN in IDS; applying the MOA on dataset; classify the dataset which are normal and abnormal activities; output value of MOA will support ANN to maximize the classification rate and the final parts involved the analysis and comparison of the optimization by using ANN supported by MOA.

This project uses the Magnetic Optimization Algorithm (MOA) in combination with Particle Swarm Optimization (PSO) to determine the accuracy of Intrusion Detection System (IDS). The simulation method applied in MATLAB toolkit yielded a comparison of classification rates using MOA, PSO, and a combination of PSO and MOA. Those optimization approaches lead to different outcomes.

As a conclusion, the hybrid of PSOMOA produce highest accuracy and classification rate for high numbers of training samples. The combination optimization method proven that the MOA can support ANN and PSOMOA is a reliable technique which perform high accuracy and efficiency due to its function like a magnetic that can attract more particles. The classification rate of hybrid of PSOMOA achieves 99.5%, PSO achieves 98% and MOA achieves 98.5%.

Acknowledgement

This research is fully supported by Fundamental Research Grant Scheme (FRGS), which help in completing the research in viable and efficient.

References

1. Kumar Gulshan and Kumar Krishan, “The Use of Artificial-Intelligence-Based Ensembles for Intrusion Detection: A Review”, Hindawi Publishing Corporation, 2012.
2. Noor Suhana Sulaiman, Nur Sukinah Aziz, Nooraida Samsudin, Wan Ainul Alyani Wan Mohamed, “Big Data Analytic of Intrusion Detection System” International Journal of Advanced Trends in Computer Science and Engineering, 2020.
3. Amin Dastanpour, Suhaimi Ibrahim, Reza Mashinchi and Ali Selamat, “Using Gravitational Search Algorithm to Support Artificial Neural Network in Intrusion Detection System”, Smar Computing Review, Vol. 4, No. 6, December 2014.
4. SeyedAli Mirjalili, Siti Zaiton Mohd Hashim and Hossein Moradian Sardroudi, “Training FeedForward NeuralNetworks using Hybrid Particle Swarm Optimization and Gravitational Search Algorithm”, Elsevier, 2012.

5. Prajakta Solankar, Subhash Pingale and Ranjeet Singh Parihar, “Denial of Service Attack and Classification Techniques for Attack Detection”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015.
6. Noor SuhanaSulaiman, NurSukinah Aziz, NooraidaSamsudin, Wan Ainul Alyani, Azliza-Yacob, LukmanulhakimNgah, “Overview of Network Dataset and Data Mining Technique’, International Journal of Advanced Trends in Computer Science and Engineering, 2020.
7. Shi-Jinn Horng, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai and Citra Dwi Perkasa, “A Novel intrusion Detection System Based on Hierarchical Clustering and Support vector Machines”, Elsevier, 2010.
8. Yinhui Li, Jingbo Xia, Silan Zhang, Jiakai Yan, Xiaochuan Ai and Kuobin Dai, “An Efficient Intrusion System Based on Support Vector Machines and Gradually Feature Removal Method”, Elsevier, 2011.
9. WenJie Tian and JiCheng Liu, “A New Network Intrusion Detection Identification Model Research”, International Asia Conference on Informatics in Control, Automation and Robotics, 2010.
10. Mehdi Moradi and Mohammad Zulkernine, “A Neural Network Based System for Intrusion Detection and Classification of Attacks”, Natural Sciencesand Engineering Research Council of Canada (NSERC), 2004.
11. Swati Paliwal and Ravindra Gupta, “Denial-of-service, Probing & Remote to User (R2L) Attack Detection Using Genetic Algorithm”, International Journal of ComputerApplications, Vol. 60, No. 19, December 2012.
12. Megha Aggarwal and Amrita, “Performance Analysis of Different Feature Selection Methods in Intrusion Detection”, International Journal Of Scientific & Technology Research Volume 2, Issue 6, June 2013.
13. Indraneel Mukhopadhyay and Mohuya Chakraborty, “Hardware Realization of Artificial Neural Network Based Intrusion Detection & Prevention System”, Journal of Information Security, 2014.
14. Adetunmbi A.Olusola, Adeola S.Oladele and Daramola O.Abosede, “ Analysis of KDD “99 Intrusion Detection Dataset for Selection of Relevance Features”, Proceedings of the World Congress on Engineering and Computer Science, Vol. I, 2010
15. N. S. Chandolikar and V. D. Nandavadekar,”Selection of Relevant Feature for Intrusion Attack Classification by Analyzing KDD CUP 99”, MIT International Journal of ComputerScience & Information Technology, Vol.2, No. 2, August 2012.