© Universiti Tun Hussein Onn Malaysia Publisher's Office

IJIE

http://penerbit.uthm.edu.my/ojs/index.php/ijie
ISSN : 2229-838X e-ISSN : 2600-7916

The International Journal of Integrated Engineering

An Intrusion Detection System Based on Hybrid of Artificial Neural Network (ANN) 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, Teluk Kalong, Kemaman, Terengganu, 24000, MALAYSIA

*Corresponding Author

DOI: https://doi.org/10.30880/ijie.2022.14.03.016
Received 11 Jnauary 2022; Accepted 04 June 2022; Available online 20 June 2022

Abstract: Intrusion Detection System is a type of security application that protects computer and network systems. A variety of techniques have been proposed to increase IDS accuracy. This research study focuses on improving an IDS detection performance by combining an Artificial Neural Network (ANN) with a Magnetic Optimization Algorithm (MOA), with the goal of increasing the classification rate and achieving high detection accuracy in IDS. The suggested ANNMOA result demonstrated that it is possible to improve IDS accuracy by up to 98.5 percent.

Keywords: Artificial neural network, magnetic optimization algorithm, intrusion detection system, KDD Cup 99, classification

1. Introduction

People nowadays utilize the Internet as their medium of interaction, banking, and cultural networking. They had no idea that their information had been compromised. Meanwhile, businesses are investing heavily in network security to safeguard subtle data from attackers and guarantee that data transfer is secure. On Internet of Things, the number of users, items, and gadgets connected to each other over the Internet (IoT). Because of online transactions, cloud solutions for storing data such as credential data and paperless transactions have seen a rising trend. When most people make an online purchase, check their email, or go to the shop, they are unconcerned about their identities being stolen (Muhirwe & White, 2016). Cyber-attacks have increased the vulnerability of people and organizations, and they have had a significant detrimental impact (Mohannadi, 2018). Consumers are at danger of public network or Internet security breaches, such as stolen online credentials, unprotected communication between senders and receivers, and illegal communication session access, as a result of all of these online technology requirements (Noor et al., 2021). Phishing and online fraud are just a few of the risks that users face on a regular basis (Garba et. al.,2020). Indeed, given the current rate of technical advancement in the online world, IoT-based systems are growing more susceptible. Until until, network intrusions were detected using an Intrusion Detection System (IDS) that monitored network traffic. Intrusion detection systems (IDS) are critical security components for protecting networks from malicious activity. An intrusion detection system may alternatively be thought of as "an effective security element capable of detecting, preventing, and responding to computer assaults" (Kumar et al, 2012). Previously, intrusion detection depended on examining network traffic, records, and system events (Noor et. al., 2020). DS detects using two methods: signature recognition and anomaly detection. Signature recognition detects intrusions based on known attack architecture, whereas anomaly detection evaluates typical activity aspects (Siti et. al., 2021).

The Artificial Neural Network (ANN) proved to be the easiest approach to optimize an IDS (Mukkamala, 2002). For normal and abnormal activity, the three and four level neural networks generated values of around 99.25 percent. The positive outcome of this study demonstrates the potential of ANN for increasing high efficiency of identification rate and

Corresponding author: norwahidayah@uctati.edu.my precision in IDS. However, there are several unsolved issues that must be addressed to maximize ANN in IDS. As a result, in this work, the Magnetic Optimization Algorithm (MOA) will be proposed along with a new training technique to optimize an IDS.

This chapter discusses the study's history and the research challenge statement. The various experiment studies and results obtained will be discussed in detail throughout the section.

2. Illustrations

The Intrusion Detection System was created and implemented on production networks between the end of the 1970s and the early 1980s, and it is still in use today. In recent years, intrusion detection systems (IDS) have emerged as a novel security solution for preparing for and responding to network threats (Asmaa et. al., 2011). An intrusion detection system's (IDS) job is to keep track of network traffic and target packets that would exploit known security flaws. A potential attacker may disguise its harmful activities with side effects that cause the system to behave strangely. The network dataset has been widely utilized in network research. Network datasets, such as KDD Cup 99, have major challenges that result in several difficulties, such as increased data processing and transmission time and an increased false alarm rate in attack detection, resulting in injury and an unsafe environment for online users, including IDS datasets. KDD Cup 99 datasets are represented in Matlab Simulink as poor and excellent packets (Noor et. al. 2020). Tracking individuals and things as they travel across the network is one of the problems for intrusion detection in a network setting. The shortcomings of Intrusion Detection Systems (IDS) in detecting abnormal activities amid the normal are a significant challenge in researcher effort. Several Artificial Intelligence (AI) approaches have been developed to address the issues (Danstanpour et. al., 2014). The goal of AI is to find and learn, and then adapt to changing situations throughout time. Artificial Neural Networks are the most widely utilized AI approaches for assault detection (ANN).

The classification and regression problems can both be solved with ANN. However, ANN has a drawback in terms of its ability to learn by observing a dataset. (Dastanpour et. al., 2014). The purpose of the Feed Forward Neural Network (FNN) learning process is to find the best combination of connection weight and biases to obtain the least amount of error. FNN, on the other hand, frequently converge to locations that are the best answer locally but not globally. Simulated Annealing (SA), Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Magnetic Optimization Algorithm (MOA), and Differential Evaluation (DE) are some of the Heuristic Optimization approaches that have been developed to train FNN (Mirjalili et. al., 2012). According to the (Mirjalili et. al., 2012) It has some of the downsides of those optimization approaches, such as poor convergence rates.

Recently, Multi-Layer Perceptron (MLP) has been increasingly popular in computational tools and has been used in a variety of applications (Mirjalili & Sadiq, 2011). Each of the output neurons' input values will be generated when the input enters the network (Ernesto et al, 2015). The weighting can be modified in the hidden layer to get a more accurate result. MLP's learning method has various drawbacks, like delayed convergence and local minimal become stuck. MLP is regarded as a flaw algorithm since it is unreliable in solving issues. Magnetic Optimization Method (MOA) is a common experience optimization algorithm used in this research to address the limitations of the Back Propagation Neural Network (BPNN) (Mirjalili & Sadiq, 2011). MOA is based on magnetic theory and can solve optimization issues accurately.

During the learning process, the aim of the Neural Network is to find the optimum combination of link weights and biases to obtain the lowest possible error. This study chose to use MOA to overcome the constraint of back propagation. According to the literature, the Magnetic Optimization Algorithm (MOA) outperforms the Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). MOA is a novel optimization approach based on magnetic field theory in physics created by (Tayarani & Akbarzadeh, 2008). In the search space, it deals with particle attraction. Each magnetic particle has a mass and magnetic field measurement due to its fitness. Acceptable magnetic particles have a stronger magnetic field and a higher mass. Electromagnetic force is one of the MOA forces in the universe. The MOA forces include a long-range effect, which means that the influence decreases as the distance between two particles increases. This force type vanishes when the distance between two particles approaches infinity. This approach suggests a means to attract each magnetic particle into a long-range force (Tayarani & Akbarzadeh, 2008). MOA may be thought of as a collection of search agents that use masses and fitness functions (Mirjalili & Sadiq, 2011). (Tayarani & Akbarzadeh, 2008) suggested a mathematically MOA that interacts in a lattice-like manner. This lattice describes which agents can exert electrical force on each other. The method begins by randomly assigning all agents to a search space. The combination of ANN and MOA is used in this research to provide high accuracy in attack detection.

3. Kdd 99 Dataset

The intrusion detection evaluation data from MIT Lincoln Laboratory - DARPA (Defense Advanced Research Projects Agency) was used in this investigation (Moradi, 2004). The dataset's sample version had over 450,000 connection records. A selection of the data containing the required attack types and an acceptable number of normal occurrences was carefully picked. The dataset is commonly used to evaluate anomaly detection algorithms. The KDD CUP '99 Dataset is split into two parts: training sets and testing sets. The training dataset contains approximately 4,900,000 vectors, each with 41 features and a normal or attack classification. The dataset's records take continuous, discrete, and symbolic formats. This project's protocol type feature represents 2 as tcp, 3 as udp, 4 as icmp, and 5 as various symbols. Furthermore, for the outcome, I used 0 for Normal and 1 for Attack. The assaults are classified as follows:

a. Denial of Service Attack (DoS): A DoS attack is when an attacker sends many pings to make the network busy and slow. As a result, the attacker can prevent a legitimate user from accessing the servers (Mahbod et. al., 2009).
b. User to Root Attack (U2R): The attacker has local access to the victim's computer and is attempting to get root access (Paliwal et. al., 2012).
c. Remote to Local Attack (R2L): The attacker did not have local access to the victim's workstation, but he attempts to get access as a user (Paliwal et al., 2012).
d. Probe Attack: Intruders attempt to obtain knowledge about the target machine in order to bypass security measures (Mahbod et. al., 2009).

Generally, most researchers employed the KDD CUP 10% Dataset, which has a total dataset size of 494,020. The distribution dataset for normal is 97280, the Probe dataset is 4107, the DoS dataset is 391458, the U2R dataset is 52, and the R2L dataset is 1124. (Aggarwal & Amrita, 2013). The distribution of intrusion types in datasets is shown in Table 1.

Table 1 – Dataset intrusion types distribution

Dataset	Normal	Probe	DoS	U2R	R2L	Total
10% KDD CUP ‘99	97280	4107	391458	52	1124	494020

The types of attacks used by Probe are satan, ipsweep, nmap, and portsweep. Aside from that, DoS attacks include back, land, Neptune, pod, smurf, and teardrop. Password guessing, ftp writes, imap, phf, multihop, warezmaster, warezclient, and spy attacks were all used in R2L. Finally, the buffer overflow, loadmodule, perl and rootkit categorized as U2R (Olusola et. al., 2010). The computer system eventually runs out of memory resources after sending several TCP packets. The Smurf attack, which sends an ICMP echo request packet to an intermediate device, is a popular form of assault. The victim's IP address is used as the source address, while the intermediate device address is used as the destination address in ICMP packets (Solankar et. al., 2015). As stated in the Neptune and Smurf attacks, a DoS attack decreases server performance by flooding ICMP traffic. As a result, detecting a DoS attack is critical for system security (Solankar et. al., 2015). In addition, in the standard format stage, one column will be added to designate each record as a result, which will be 0 for normal and 1 for attack. The goal of adding this extra row is to keep the ANN error restructuring going and understand it. Because the ANN toolbox of the MATLAB toolkit only supports data in integer form, the specified attributes in the dataset are transformed to double data type to make it compatible with it (Indraneel et. al., 2014).

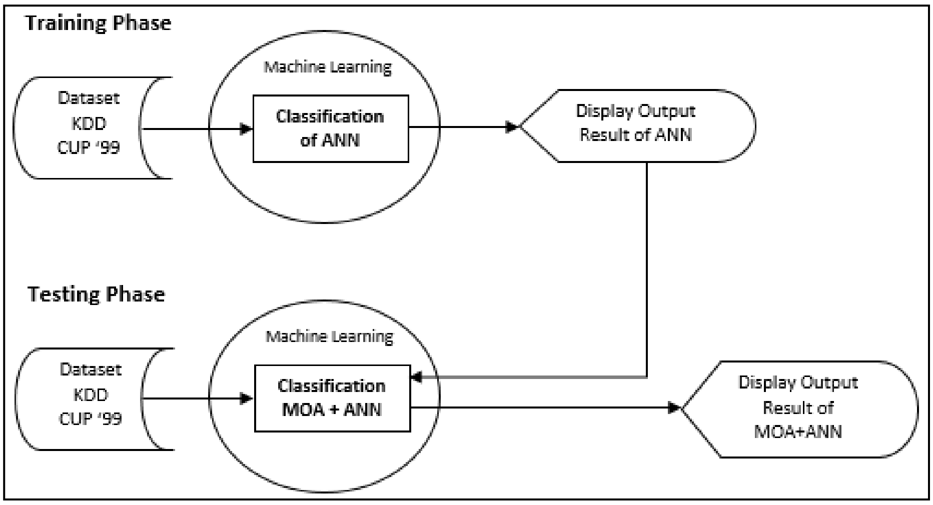

Fig. 1 – Research process flow

4. Methodology

As input values, the KDD CUP '99 dataset will be used. The KDD CUP '99 dataset has 41 features and 494020 records. This dataset contains 41 columns and 494020 rows. The data range for the ANN must be [0 1] or [-1 1]. Each KDD CUP '99 record takes one of three forms: continuous, discrete, or symbolic. Each symbol is allocated an integer code for conversion into numerical form. It is not feasible to use all the rows in the dataset because it would take too long to run. In this work, just four important dataset characteristics were chosen, and 200 rows of input values were utilized to train the ANN.

Furthermore, in the standard format step, one column will be added to identify each record, which will be 0 for normal and 1 for attack. The purpose of adding this extra row is to continue and comprehend the mistake rearrangement in ANN. Because the ANN toolbox of the MATLAB toolkit only supports data in integer form, the provided characteristics in the dataset are converted to double data type. The "protocol type" feature is transformed with values such as tcp being 2 and udp being 3. Because just 200 rows of data were utilized to test the method, not all protocol types were used for this project.

The MOA was utilized to optimize the ANN findings. MOA instructs the random agent to compute the mass value of each agent to optimize the ANN. In this work, the MOA parameters utilized were the number of agents, the maximum number of iterations, the number of training samples, the inertia weight, the lowest weight, the maximum weight, and the objective function. This study proposes a technique for training ANN to maximize IDS with MOA. To begin, this study attempts to split the dataset into two halves for training and testing. The techniques then attempt to establish a common dataset format for ANN reorganization. Following the completion of the ANN's training, the ANN will attempt to classify the KDD CUP '99 testing dataset and take the accuracy output of the system detection, which will then be plotted and monitored by the system. The MOA data input is the result of the ANN's recognition when it's finished. At this stage, MOA will try to optimize the ANN rearrangement. Finally, when the MOA has optimized the ANN results, they will be displayed and compared to the ANN result (without MOA) to better understand the effects of MOA in the ANN reorganization in the intrusion detection system using the KDD CUP '99 dataset. Figure 1 presents the basic idea as well as the entire techniques.

5. Result and Discussion

The masses determine the effectiveness of agents. The bigger the mass, the more effective the agent, the greater the attraction. As a result, the smaller masses are inefficient agents. However, greater masses take longer to seek in the population than lesser masses. In this section, the results from the various parameter settings will be compared and explained. The experiment is carried out via MOA optimization on ANN. Depending on the parameters, these algorithms will provide various results. The experiment's parameter setting has been set to masses. This section employs masses of 10, 20, and 40. Table 2 illustrates the first parameter setting by adjusting the masses to 10 and using the same setting for the remaining parameters. Figure 1 depicts the outcome of changing the masses. 2, 3, 4, 5, 6, 12, 23, 25, 26, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, and 39 are the features utilized.

By increasing the masses to 10, the initial parameter setting can lower the accuracy of MOA optimization on ANN by 40%. The mean square error (MSE) similarly falls until it reaches 0.6. According to the observations, the runtime required by employing masses 10 takes a relatively short time to compute. However, the masses utilized are incapable of producing high detection accuracy. The masses utilized can influence the detection rate since a heavier mass is more efficient, which implies the better agent has a higher attraction. The mass is used to search the universe for the finest agents. The result drops to 40% since the number of masses utilized is just 10, implying that the search space to identify the optimal agents is quite restricted.

Table 2 – MOA Parameters

Parameter MOA Values	Parameter MOA Values
Mass	10
Maximum of Iteration	200
Number of Training Samples	200
Inertia Weight	2
Minimum weight	0.5
Maximum weight	0.9
Objective Function	Maximum

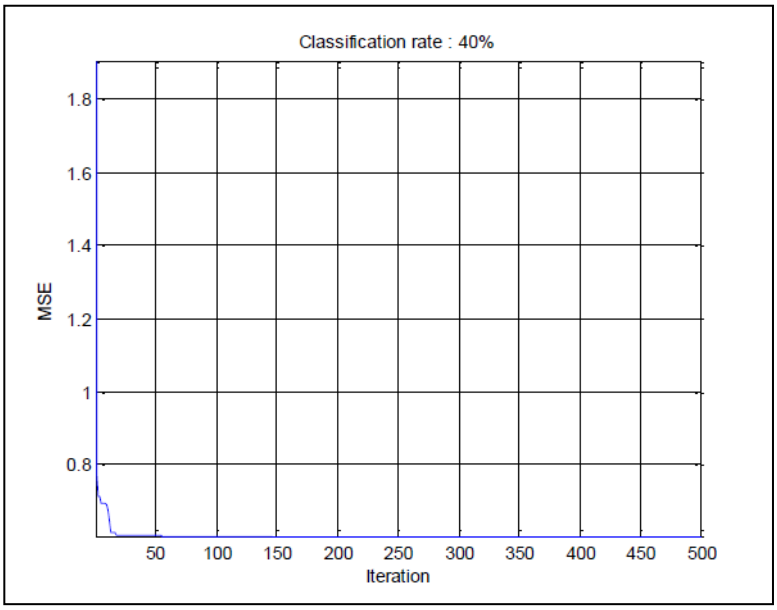

Fig. 2 – Result of ANN optimized by MOA using masses 10.

The second parameter MOA setting is used in the MOA and ANN experiment. The masses utilized are 20 and the other factors are the same. Assumed that greater masses can produce a higher categorization rate. When compared to the initial parameter setting, the categorization rate produces superior results. The runtime required is more than that of masses 10. Higher masses will take longer to run. Figure 3 depicts the classification rate obtained by utilizing the second parameter setting for moa optimization on ann. The result showed 92.5 percent accuracy with a high MSE of 0.58. When utilizing masses 20 instead of masses 10, the detection rate improves. The third parameter option is used in the moa and ANN experiments. Masses 30 were not utilized since it is the project's default value. The masses utilized are 40, and the other parameters are the same. When compared to the first and second parameter settings, the classification rate gives superior results. According to the observations, the runtime required is longer than in the prior experiment. Figure 4 shows the classification rate obtained by utilizing the second parameter setting for moa optimization on ann. The outcome is an increase in accuracy up to 98.5 percent with a low MSE of 0.7. When compared to the masses 30 utilized, the classification rate improves. The detection classification rate is influenced by greater masses.

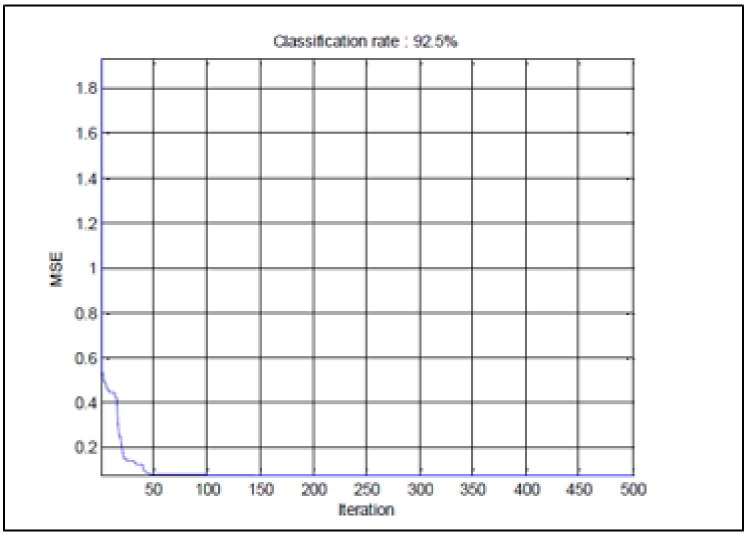

Fig. 3 – Result of ANN optimized by MOA using masses 20.

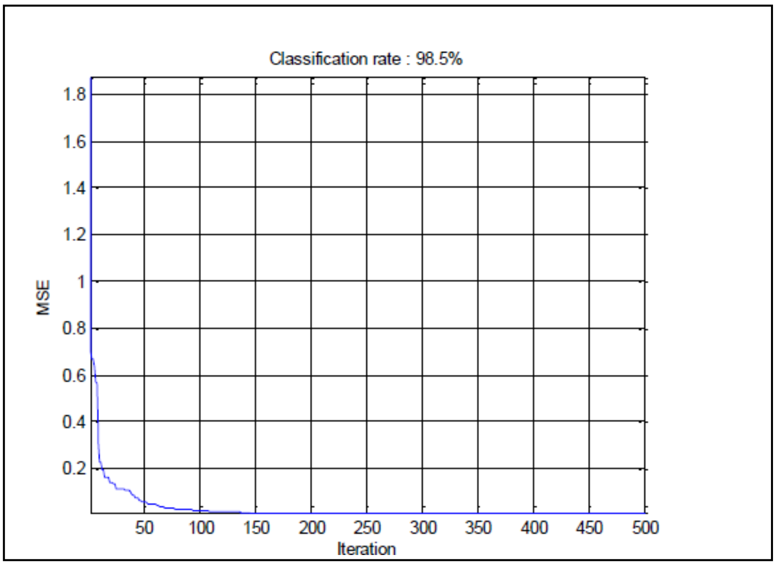

Fig. 4 – Result of ANN optimized by MOA using masses 40.

6. Conclusion

Contributions were made because of studying and analyzing the nature of the KDD dataset. The parameter is utilized to get a high classification rate by choosing the best features. The job of the research seeks to provide data figures a key function in improvement methods. Adopting a learning approach to solve optimization issues quickly and accurately by implementing the Hybrid Artificial Neural Network (ANN) and Magnetic Optimization Algorithm (MOA) using building a training technique will provide three primary benefits: improved training times, high accuracy, higher detection rate, and improved generalization by reducing overfitting.

Acknowledgement

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

References

[1] Jackson Muhirwe and Nathan White, Cybersecurity Awareness and Practice of Next Generation Corporate Technology Users, Issues Inf. Syst., vol. 17, 2016.

[2] Hamad AL-Mohannadi, Irfan Awan, Jassim Al Hamar, Yousef Al Hamar, Mohammad Shah, and Ahmad Musa, Understanding Awareness of Cyber Security Threat Among IT Employees, 2018.

[3] Adamu A. Garba, Mahezyah Md Siraj, Siti Hajar Osman and M. A. Musa, A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach, A Study Cybersecurity Aware. Among Students Yobe State Univ. Niger. A Quant. Approach, 2020.

[4] Noor Suhana Sulaiman, Akhyari Nasir, Wan Roslina Wan Othman, Syahrul Fahmy Abdul Wahab, Nur Sukinah Aziz, Azliza Yacob, Nooraida Samsudin, Intrusion Detection System Techniques: A Review, IOP Journal of Physics: Conference Series, 2021.

[5] Kumar Gulshan and Kumar Krishan, The Use of Artificial-Intelligence-Based Ensembles for Intrusion Detection: A Review, Hindawi Publishing Corporation, 2012.

[6] Noor Suhana Sulaiman, Nur Sukinah Aziz, Nooraida Samsudin and Wan Ainul Alyani Wan Mohamed, Big Data Analytic of Intrusion Detection System, International Journal of Advanced Trends in Computer Science and Engineering, 2020.

[7] Siti Norwahidayah, Nurul Farahah, Noraniah, Ainal Amirah, Nur Liyana Zakaria and Noor Suhana, Performances of Artificial Neural Network (ANN) and Particle Swarm Optimization (PSO) Using KDD Cup ‘99 Dataset in Intrusion Detection System (IDS), IOP Journal of Physics: Conference Series, 2021.

[8] Mukkamala Srinivas, Intrusion Detection using Neural Networks and Support Vector Machine. Proceedings of the 2002 IEEE International Honolulu, 2002.

[9] Asmaa Shaker Ashoor and Sharad Gore, Importance of Intrusion Detection System (IDS), International Journal of Scientific Engineering Research, 2011.

[10] Noor Suhana Sulaiman, Nur Sukinah Aziz, Nooraida Samsudin, Wan Ainul Alyani, Azliza Yacob and Lukmanulhakim Ngah, Overview of Network Dataset and Data Mining Technique, International Journal of Advanced Trends in Computer Science and Engineering, 2020.

[11] Amin Dastanpour, Suhaimi Ibrahim, Reza Mashinchi and Ali Selamat, Using Gravitational Search Algorithm to Support Artificial Neural Network in Intrusion Detection System, Smart Computing Review, 2014.

[12] Seyedali Mirjalili and Ali Safa Sadiq, Magnetic Optimization Algorithm for Training MultiLayer Perceptron, IEEE, 2011.

[13] Mohammad Tayarani Najaran and Mohammad-R. Akbarzadeh-T, Magnetic Optimization Algorithms a New Sysnthesis, IEEE, 2008.

[14] Jose Ernesto Luna Dominguez and Anabelem Soberanes Martin, Intrusion Detection Pattern Recognition Using an Artificial neural Network, International Journal of Engineering Science, and Innovative Technology, 2015.

[15] Mehdi Moradi and Mohammad Zulkernine, A Neural Network Based System for Intrusion Detection and Classification of Attacks, Natural Sciences and Engineering Research Council of Canada (NSERC), 2004

[16] 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.

[17] Mahbood Tavallaee, Ebrahim Bagheri, Wei Lu and Ali A. Ghorbani, A Detailed Analysis of the KDD CUP 99 Dataset, IEEE, 2009.

[18] 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, 2012.

[19] 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.

[20] 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.

[21] Indraneel Mukhopadhyay and Mohuya Chakraborty, Hardware Realization of Artificial Neural Network Based Intrusion Detection & Prevention System, Journal of Information Security, 2014.