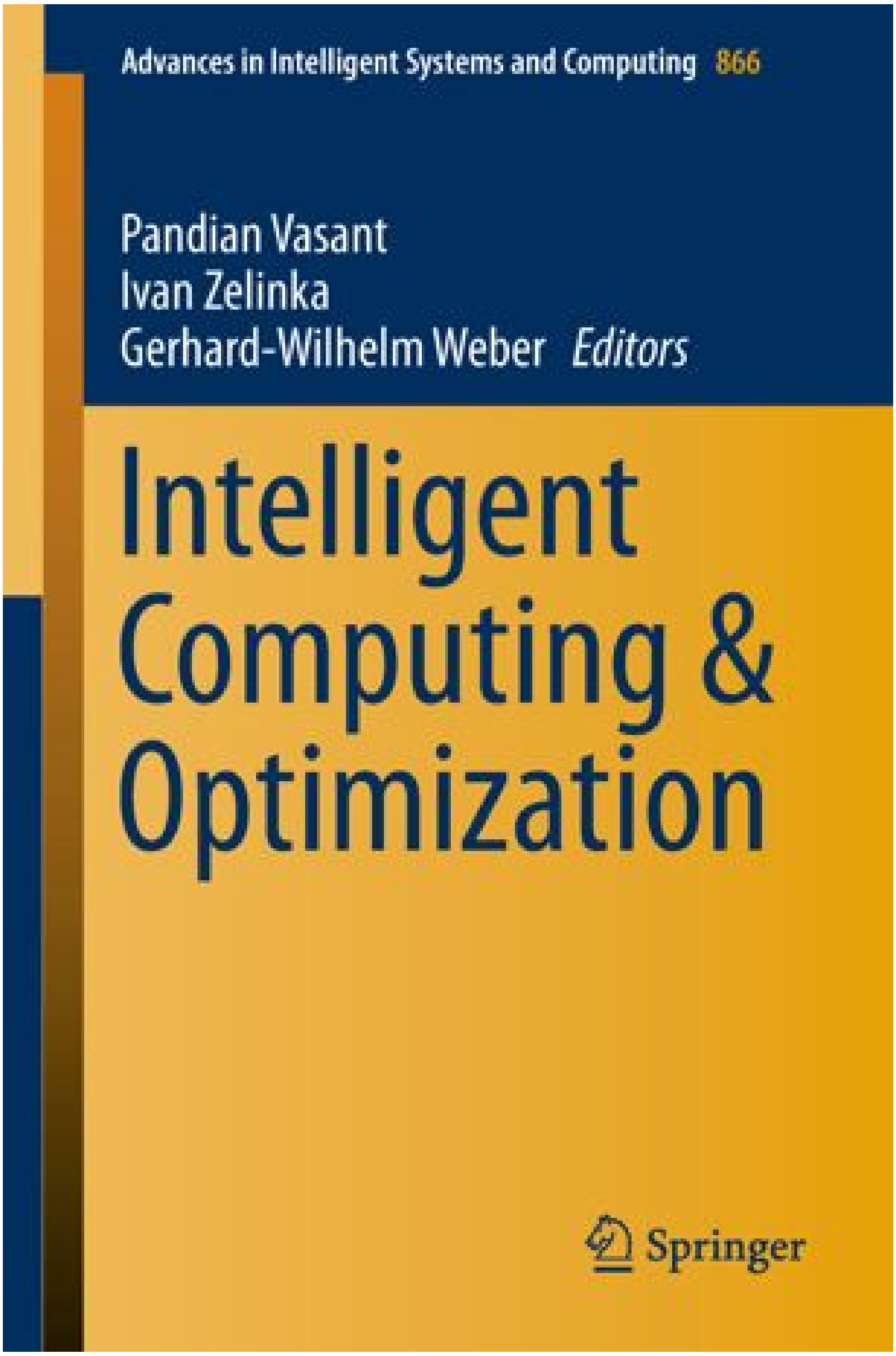

Intelligent Computing & Optimization

Editors: **Vasant**, Pandian, **Zelinka**, Ivan, **Weber**, Gerhard-Wilhelm (Eds.)

Pandian Vasant · Ivan Zelinka
Gerhard-Wilhelm Weber
Editors

Intelligent Computing & Optimization

Springer

Editors
Pandian Vasant
Department of Fundamental and Applied Sciences
Universiti Teknologi Petronas
Tronoh, Perak, Malaysia

Gerhard-Wilhelm Weber
Institute of Applied Mathematics
METU
Ankara, Ankara, Turkey

Ivan Zelinka
Faculty of Electrical Engineering and Computer Science
VŠB TU Ostrava
Ostrava, Czech Republic

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-030-00978-6 ISBN 978-3-030-00979-3 (eBook)
https://doi.org/10.1007/978-3-030-00979-3

Library of Congress Control Number: 2018955576

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The first edition of the International Conference on Intelligent Computing and Optimization (ICO 2018) will be held during October 4–5, 2018, at Hard Rock Hotel Pattaya in Pattaya, Thailand. The objective of the international conference is to bring together the global research scholars, experts, and scientists in the research areas of Intelligent Computing and Optimization from all over the world to share their knowledge and experiences on the current research achievements in these fields. This conference provides a golden opportunity for global research community to interact and share their novel research results, findings, and innovative discoveries among their colleagues and friends. The proceedings of ICO 2018 is published by Springer (**Advances in Intelligent Systems and Computing**) and indexed by DBLP, EI, Google Scholar, Scopus, and Thomson ISI.

For this edition, the conference proceedings covered the innovative, original, and creative research areas of sustainability, smart cities, meta-heuristics optimization, cyber security, block chain, big data analytics, IoTs, renewable energy, artificial intelligence, power systems, reliability, and simulation. The authors are very enthusiastic to present the final presentation at the conference venue of Hard Rock Hotel in Pattaya, Thailand. The organizing committee would like to sincerely thank all the authors and the reviewers for their wonderful contribution for this conference. The best and high-quality papers have been selected and reviewed by International Program Committee in order to publish in **Advances in Intelligent System and Computing** by Springer.

ICO 2018 will be an eye-opener for the research scholars across the planet in the research areas of innovative computing and novel optimization techniques and with the cutting-edge methodologies. This conference could not have been organized without the strong support and help from the staff members of Hard Rock Hotel Pattaya, Springer, Click Internet Traffic Sdn Bhd, and the organizing committee of ICO 2018. We would like to sincerely thank Prof. Igor Litvinchev (Nuevo Leon State University (UANL), Mexico), Prof. Nikolai Voropai (Energy Systems Institute SB RAS, Russia), and Waraporn Nimitsuphachaisin (Hard Rock Hotel Pattaya) for their great help and support in organizing the conference.

We also appreciate the fruitful guidance and support from Prof. Gerhard Wilhelm Weber (Poznan University of Technology, Poland; Middle East Technical University, Turkey), Prof. Rustem Popa ("Dunarea de Jos" University in Galati, Romania), Prof. Valeriy Kharchenko (Federal Scientific Agroengineering Center VIM, Russia), Dr. Wonsiri Punurai (Mahidol University), Prof. Milun Babic (University of Kragujevac, Serbia), Prof. Ivan Zelinka (VSB-TU Ostrava, Czech Republic), Dr. Jose Antonio Marmolejo (Universidad Anahuac Mexico Norte, Mexico), Prof. Gilberto Perez Lechuga (University of Autonomous of Hidalgo State, Mexico), Prof. Ugo Fiore (Federico II University, Italy), Prof. Weerakorn Ongsakul (Asian Institute of Technology, Thailand), Prof. Rui Miguel Silva (Portugal), Mr. Sattawat Yamcharoew (Sparrow Energy Corporation, Thailand), Mr. K. C. Choo (CO2 Networks, Malaysia), and Dr. Vinh T. Le (Ton Duc Thang University, Vietnam).

Our book of proceedings provides a premium reference to graduate and post-graduate students, decision makers, and investigators in private domains, universities, traditional and emerging industries, governmental and non-governmental organizations, in the fields of various operational research, AI, geo- and earth sciences, engineering, management, business, and finance, where ever one has to represent and solve uncertainty-affected practical and real-world problems. In the forthcoming times, mathematicians, statisticians, computer scientists, game theorists and economists, physicist, chemists, representatives of civil, electrical, and electronic engineering, but also biologists, scientists on natural resources, neuroscientists, social scientists, and representatives of the humanities, are warmly welcome to enter into this discourse and join the collaboration for reaching even more advanced and sustainable solutions. It is well understood that predictability in uncertain environments is a core request and an issue in all fields of engineering, science, and management. In this regard, this proceedings book is following a quite new perspective; eventually, it has the promise to become very significant in both academia and practice and very important for mankind!

Finally, we would like to sincerely thank Dr. Thomas Ditzinger, Dr. Almas Schimmel, and Ms. Parvathi Krishnan of Springer for the wonderful help and support in publishing ICO 2018 conference proceedings in **Advances in Intelligent Systems and Computing**.

October 2018

Pandian Vasant
Gerhard-Wilhem Weber
Ivan Zelinka

Contents

Network Intrusion Detection Framework Based on Whale Swarm Algorithm and Artificial Neural Network in Cloud Computing

Ahmed Mohammed Fahad(✉), Abdulghani Ali Ahmed, and Mohd Nizam Mohmad Kahar

Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, 26300 Kuantan, Malaysia
ahmedsipher2010@yahoo.com, {abdulghani,mnizam}@ump.edu.my

Abstract. Cloud computing is a rapidly developing Internet technology for facilitating various services to consumers. This technology suggests a considerable potential to the public or to large companies, such as Amazon, Google, Microsoft and IBM. This technology is aimed at providing a flexible IT architecture which is accessible through the Internet for lightweight portability. However, many issues must be resolved before cloud computing can be accepted as a viable option to business computing. Cloud computing undergoes several challenges in security because it is prone to numerous attacks, such as flooding attacks which are the major problems in cloud computing and one of the serious threat to cloud computing originates came from denial of service. This research is aimed at exploring the mechanisms or models that can detect attacks. Intrusion detection system is a detection model for these attacks and is divided into two-type H-IDS and N-IDS. We focus on the N-IDS in Eucalyptus cloud computing to detect DDoS attacks, such as UDP and TCP, to evaluate the output dataset in MATLAB. Therefore, all technology reviews will be solely based on network traffic data. Furthermore, the H-IDS is disregarded in this work.

Keywords: IDS · WOA · ANN · TUIDS · Cloud computing

1 Introduction

A cloud refers to a distinct IT environment that is designed to remotely provide scalable and measured IT resources [1]. This term originated as a metaphor for the Internet, which is a network of networks that provide a remote access to a set of decentralised IT resources [2]. The symbol of a cloud is commonly used to represent the Internet in various specifications and mainstream documentations of web-based architectures before cloud computing has become a formalised IT industry sector [3]. Figure 1, illustrates the importance of cloud computing in remote services and virtual desktop applications [4].

P. Vasant et al. (Eds.): ICO 2018, AISC 866, pp. 56–65, 2019.
https://doi.org/10.1007/978-3-030-00979-3_6

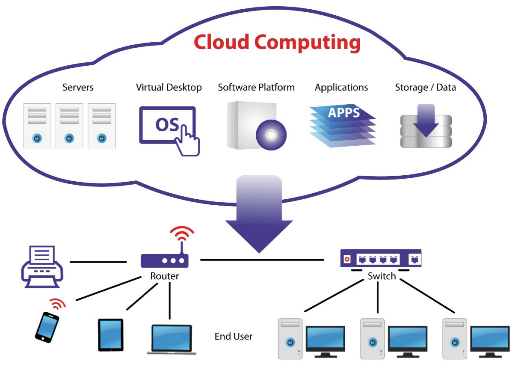

Fig. 1. Cloud computing.

A crucial aspect of cloud security is detecting DDoS attacks [5] and intrusions that disrupt the resources of end-users or organisations [6]. An N-IDS can detect these types of attacks. However, the N-IDS in cloud computing is irrelevant if the attack classifier is inaccurately written [7]. A DDoS classifier in machine learning is neural networks. Several important studies have proposed various ANN-based machine learning classifiers against DDoS in cloud computing [8]. However, considerable attention for accurate classification and reduction of false alarms remains necessary [9]. Hence, this work is aimed at proposing a new model, namely, WOA-ANN, to detect UDP/TCP flooding attacks in the N-IDS in cloud computing. To reduce the false alarm of the N-IDS system, the WOA-ANN model is used to enhance the accuracy of the N-IDS by improving the analysis of network traffic which will be generated by our cloud testbed. We compare the proposed model with existing works using MATLAB to evaluate and compare their efficiency. At the 2014 Black Hat conference, a pair of testers from Bishop Fox demonstrated the pooling of a free-tier public cloud service VM into a mini botnet that could mine bitcoin cryptocurrencies and potentially perform DDoS or password cracking [10]. Moreover, the qualities that make the public VM useful, that is, scalability, ease-of-use and stewardship by high-profile vendors, make this technology an ideal platform for staging DDoS attacks [11].

2 Proposed Framework

Whales are the largest mammals in the world. An adult whale typically measures 30 m in length [12]. Several whale species include killer, Minke, Sei, humpback, right, finback and blue. Whales, as a predator, never sleep because they breathe on the ocean surface. These animals are intelligent and show emotions. Hof and Van Der Gucht highlighted that whales have brain cells, namely, spindle cells, in which are common in humans. These cells control emotions and social behaviours in humans. The number of spindle cells in whales is twice as much as that in an adult human; therefore, whales can think, learn, judge and communicate. For example, killer whales can create their own dialect.

Most whales live in groups. A killer whale can live in a group in its lifetime [13]. Figure 2 exhibits the largest baleen whale called humpback. Its size is comparable to that of a school bus. It typical preys on krill and small fish herds [14]. Its hunting method is called bubble-net feeding in which it hunts preys that are close to the surface. This method is accomplished by creating distinctive bubbles along a circle or a '9'-shaped path. Goldbogen et al. studied this interesting behaviour using tag sensors. A total of 300 tag-derived bubble-net feeding events were captured. These authors discovered that whales use 'upward-spiral' and 'double-loop' manoeuvre patterns.

For the 'upward-spiral' pattern, humpback whales dive 12 m below the surface and create bubbles in a spiral shape around the prey. Subsequently, they swim up towards the ocean surface. The latter pattern consists of three stages: coral loop, lob tail and capture loop. In the current work, this unique spiral bubble-net feeding manoeuvre pattern was used for optimisation.

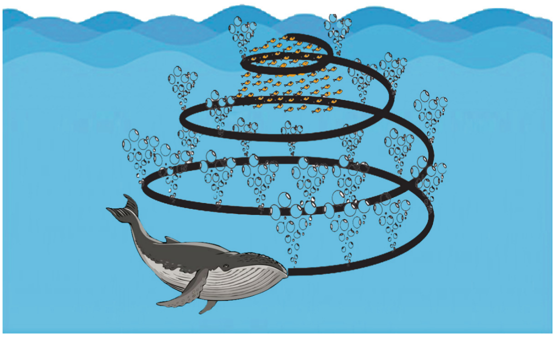

Fig. 2. WOA and bubble movement.

The mathematical models of encircling preys, spiral bubble-net feeding manoeuvre and searching for preys were outlined. The WOA algorithm was then reported. Humpback whales are aware of the location of their preys whilst hunting. The current best candidate solution is assumed as the target prey in the WOA algorithm because the location of the optimal design in the search space is unknown. The positions of other search agents are updated by defining the optimal search agent. This behaviour can be explained by the following equations:

$$\vec{X}(t+1) = \vec{X}^*(t) - \vec{B}.\vec{S} \tag{1}$$

$$\vec{S} = \left|\vec{K}.\vec{X}^*(t) - \vec{X}(t)\right| \tag{2}$$

where t is the current iteration, and are the coefficient vectors, is the position vector of the current best solution obtained and is the position vector. Here, is updated after iterations and are computed as

$$\overrightarrow{B} = 2\overrightarrow{b}.\overrightarrow{r} - \overrightarrow{b} \tag{3}$$

where decreases from 2 to 0 during the iterative phase, and is a random vector between [0, 1]. The rationale behind Eq. (2). Figure 6 explain The new position (X, Y) of a search agent is updated on the basis of the current best position (X^*, Y^*). The locations of the optimal agent can be manipulated by adjusting the and vectors. Any position that is located within the search space is reachable by using the random vector, as displayed in Fig. 3, which simulates the encircling prey movement of a whale. The same method can be applied to high-dimensional problems.

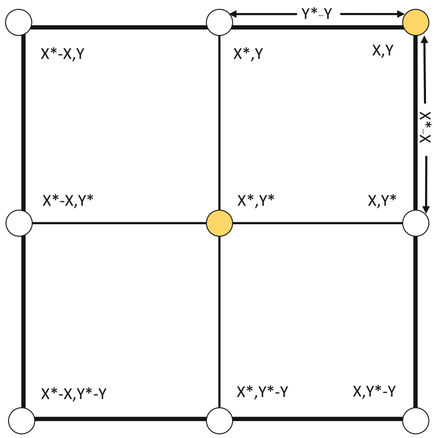

Fig. 3. position vectors and their possible next locations (X^* is the best solution obtained so far).

2.1 Bubble-Net Attacking Method (Exploitation Phase)

The bubble-net strategy can be performed using the following approaches:

1. Shrinking encircling mechanism: This strategy is achieved via reducing the value of in Eq. (1) from 2 to 0 during the iterative procedure. The new position of a search agent can then be identified by setting the random values in [−1, 1].

Figure 4, presents several possible solutions (X, Y) that can be obtained by setting $0 \leq K \leq 1$.

2. Spiral updating position: In Fig. 8, the distance between (X, Y) and (X^*, Y^*) is calculated first. A spiral equation is then established to represent the helix-shaped movement:

$$\vec{X}(t+1) = S.e^{ml}.\cos(2\pi l) + \vec{X}^*(t). \tag{4}$$

where indicates the distance of the ith whale to the prey, m is a constant that defines the shape of the logarithmic spiral and l is a random number within the range [−1, 1]. In general, a humpback whale swims around the prey within a shrinking circle, following the spiral-shaped path. A probability of 50% is prescribed on activating either the shrinking encircling mechanism or the spiral model whilst updating the whale position to model this condition.

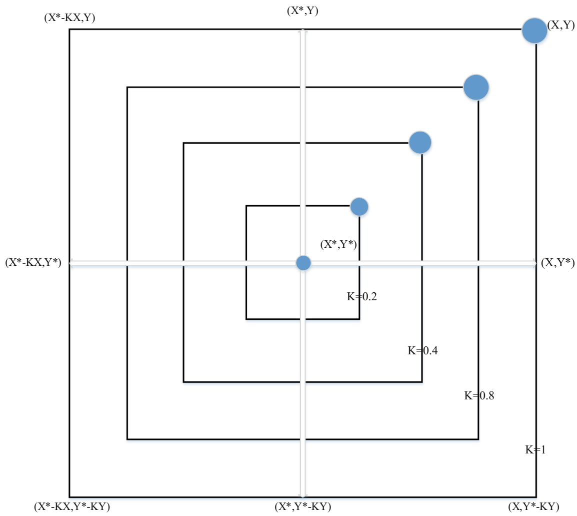

Fig. 4. Possible solutions (X, Y).

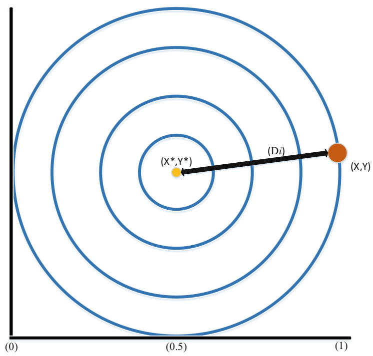

Fig. 5. Distance between (X, Y) and (X^*, Y^*).

The WOA algorithm is initialized using a set of random solutions. For each iteration, the positions of the search agents are updated based on a randomly selected search agent or the current best solution, depending on | | (Fig. 5).

Theoretically, WOA is a global optimizer because it contains exploration and exploitation capabilities. Moreover, the current hypercube mechanism defines a search space in near the optimal solution, thus permitting other search agents to search for the current best record within the domain. The mathematical model of the adaptive version of the WOA algorithm is

$$\vec{X}(t+1) = \begin{cases} \vec{X}^*(t) - \vec{B}.\vec{S} & if \quad \ell < 0.5 \\ \vec{S}'.e^{ml}\cos(2\pi l) + \vec{X}^*(t) & if \quad \ell \geq 0.5 \end{cases} \tag{5}$$

where is a random number between [0, 1]. In certain cases, a humpback whale searches for a prey randomly.

2.2 Searching for Prey (Exploration Phase)

The method can be adopted by using a similar approach of varying the vector to search for a prey (i.e. exploration). In the random method, with random values greater than or less than 1 is used to ensure that each search agent is far from the reference. Whale. Here, the position is updated randomly in accordance with the randomly selected search agent. The global search operation in WOA can be performed by applying this mechanism and setting | | > 1. The corresponding mathematical model is:

$$\vec{S} = \left|\vec{K}.\vec{X}_{rand}(t) - \vec{X}(t)\right| \tag{6}$$

$$\vec{X}(t+1) = \vec{X}_{rand}(t) - \vec{B}.\vec{S} \tag{7}$$

3 Classifier Design

In practice, a smooth transition between exploration and exploitation is feasible. Here, several iterations are allocated exploration (| | ≥ 1), whereas the remaining iterations are dedicated for exploitation (| | < 1). In WOA, only two main adjustable internal parameters are available. The current work considers a simple version of WOA by neglecting the other evolutionary operations that mimic the real behavior of humpback whales. Therefore, hybridization with evolutionary search schemes can be further explored (Fig. 6).

The average values obtained from the fitness function are considered those of the candidate solutions. The value of this fitness function is verified during the iteration until a new best value is found. The attribute that provides a minimum error value is selected to complete the selection and evaluation processes. The flow of the proposed method is as follows:

$$\mathrm{E(i) = wTrain.TrainData.E + wTest.TestData.E} \tag{8}$$

where wTrain and wTest are the heights to be used for training and test data. The error values obtained from the training and test data will be used to calculate the fitness function. In the proposed method, wTrain: 0.7 and wTest: 0.3 are considered. E(i) denotes the fitness values obtained at the end of three runs. Figure 8 depicts the method

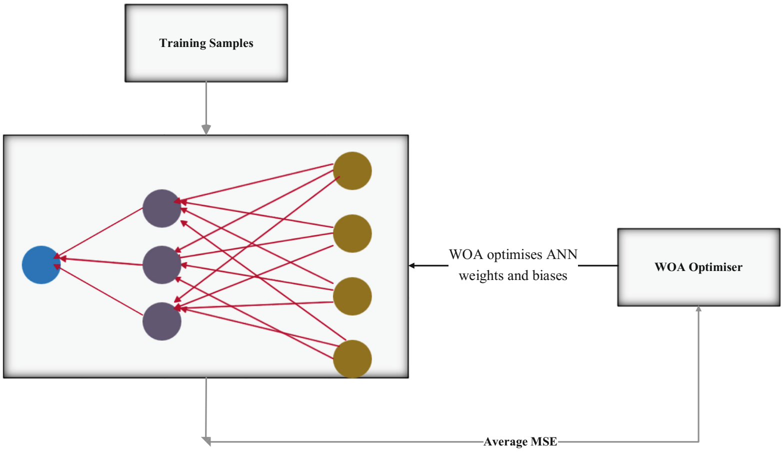

Fig. 6. Process for collecting dataset and designing a classifier.

used by WOA to feed the weights and biases and produce additional training samples efficiently.

3.1 BFGS Quasi-Newton Backpropagation

Newton's method is an alternative to conjugate gradient methods used for fast optimization. The basic step of Newton's method is:

$$X_{k+1} = X_k - A_k^{-1} g_k \tag{9}$$

where is the Hessian matrix (second derivatives) of the performance index at the current values of the weights and biases. Newton's method frequently converges faster than conjugate gradient methods. However, computing the Hessian matrix for feed-forward neural networks is complex and costly. A class of algorithms is based on Newton's method and does not require calculating the second derivatives. These methods are called quasi-Newton (or secant). They update an approximate Hessian matrix at each iteration of the algorithm. The update is computed as a function of the gradient. This algorithm requires more computation in each iteration and more storage than the conjugate gradient methods, although it generally converges in few iterations. The approximate Hessian must be stored, and its dimension is n × n, where n is equal to the number of weights and biases in the network. For large networks, using the conjugate gradient algorithms is favorable.

4 Model for N-IDS In-Eucalyptus Cloud Computing

The proposed model is aimed at synthesizing the Eucalyptus cloud as the N-IDS that analyses the generated traffic and blocks the TCP/UDP flooding and Smurf DDoS attack. A TUIDS DDoS dataset is prepared using the TUIDS testbed architecture with a demilitarized zone (DMZ); hosts are divided into several VLANs, where each VLAN belongs to an L3 or L2 switch inside the network. The attackers are placed in wired and wireless networks with reflectors, but the target is placed inside the internal network. The target generates low- and high-rate DDoS traffics. We consider real-time low- and high-rate DDoS attack scenarios for both datasets during our experiments. However, a low-rate attack does not consume all computing resources on the server or bandwidth of the network that connects the server to the Internet. Hence, a real low-rate DDoS attack scenario contains attack and attack-free traffics. We mix low-rate attack and legitimate traffics during our experiment to prepare the real low-rate DDoS attack scenarios in the TUIDS DDoS dataset (Fig. 7).

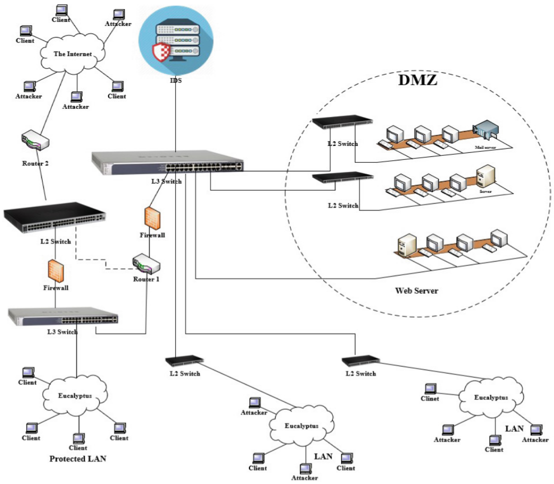

Fig. 7. New pre-processor rule structure in Eucalyptus cloud computing.

Many experiments have been conducted in this work to empirically demonstrate the impact of methodological factors, as discussed in Sect. 4.3.2. The experiments can be summarized as follows: General observations: exploring classifier performance and validation methods. Performance on original datasets: providing a benchmark that is used to compare the results obtained from subsequent experiments. Removing new attacks from the test set: this experiment is conducted to determine.

5 Classifier Process in MATLAB

We offer three specific benefits of classifier combinations. Statistical: if the amount of training data insufficiently models the hypothesis space with one classifier, then the combined knowledge of an ensemble of classifiers may reach accurate predictions. 2. Computational: algorithms can be trapped in local optima and finding the global optimum may be computationally expensive. However, executing several local search algorithms from different starting points and combining them may be favorable.

A hybrid classifier is developed in MATLAB using our dataset. First, we must perform the normalization process for the dataset. Then, the dataset will have been delivered to the training and testing sets in the following proportions: 70% training and 30% testing. The target will be TCP, UDP and Smurf attacks. The results are validated through evaluation which was derived from the machine learning metrics (Fig. 8).

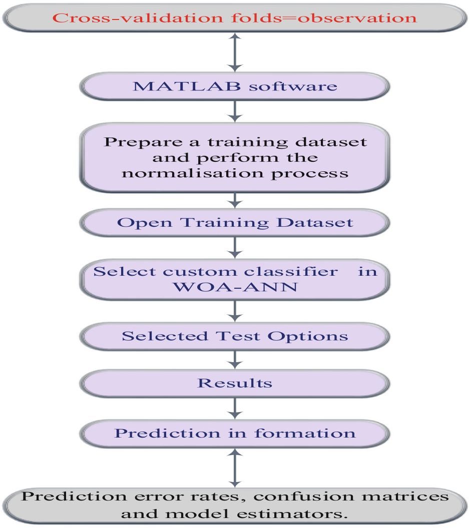

Fig. 8. WOA classifier test using MATLAB.

6 Conclusions

This work proposes a new classifier design based on a hybrid artificial neural network and whale swarm algorithm to feed the ANN weights and biases. However, the model cannot function without a derivative dataset. This dataset is derived from our testbed design based on a developed TUIDS network topology over the Eucalyptus cloud computing. In the N-IDS, sensing is used in real time for the normal and upnormal traffic DDoS attacks through Snort. The log-output from the dataset has been analyzed in MATLAB.

Acknowledgments. This work was supported by the Faculty of Computer System and Software Engineering, Universiti Malaysia Pahang under FRGS Grant No. RDU160106 and RDU Grant No. RDU160365.

References

1. Rittinghouse, J.W., Ransome, J.F.: Cloud Computing: Implementation, Management, and Security. CRC press, Boca Raton (2016)

2. Ahmed, A.A., Jantan, A., Ali, G.A.: A potent model for unwanted traffic detection in QoS network domain. JDCTA **4**, 122–130 (2010)
3. Kaul, S., Sood, K., Jain, A.: Cloud computing and its emerging need: advantages and issues. Int. J. Adv. Res. Comput. Sci. **8**(3) (2017)
4. Sultan, N.: Cloud computing for education: a new dawn? Int. J. Inf. Manag. **30**(2), 109–116 (2010)
5. Mirkovic, J., Reiher, P.: A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput. Commun. Rev. **34**(2), 39–53 (2004)
6. Elejla, O.E., Jantan, A.B., Ahmed, A.A.: Three layers approach for network scanning detection. J. Theor. Appl. Inf. Technol. **70**(2) (2014)
7. Ahmed, A.A.: Investigation model for DDoS attack detection in real-time. Int. J. Softw. Eng. Comput. Sci. (IJSECS) **1**, 93–105 (2015)
8. Ahmed, A.A., Jantan, A., Wan, T.-C.: Filtration model for the detection of malicious traffic in large-scale networks. Comput. Commun. **82**, 59–70 (2016)
9. Rowland, C.H., Rhodes, A.L.: Method and system for reducing the false alarm rate of network intrusion detection systems. ed: Google Patents (2011)
10. Nanavati, M., Colp, P., Aiello, B., Warfield, A.: Cloud security: a gathering storm. Commun. ACM **57**(5), 70–79 (2014)
11. Ahmed, A.A., Sadiq, A.S., Zolkipli, M.F.: Traceback model for identifying sources of distributed attacks in real time. Secur. Commun. Netw. **9**(13), 2173–2185 (2016)
12. Mirjalili, S., Lewis, A.: The whale optimization algorithm. Adv. Eng. Softw. **95**(Supplement C), 51–67 (2016)
13. Mirjalili, S., Lewis, A.: The whale optimization algorithm. Adv. Eng. Softw. **95**, 51–67 (2016)
14. Aljarah, I., Faris, H., Mirjalili, S.: Optimizing connection weights in neural networks using the whale optimization algorithm. Soft Comput. **22**(1), 1–15 (2018)

Author Index

P. Vasant et al. (Eds.): ICO 2018, AISC 866, pp. 573–575, 2019.
https://doi.org/10.1007/978-3-030-00979-3