THE DETECT DOS ATTACK FROM NETWORK TRAFFIC USING GRAY WOLF OPTIMIZATION ALGORITHM

Article *in* Journal of Engineering Science and Technology · December 2020

CITATION
1

READS
240

2 authors:

Muna M.T Jawhar
University of Mosul
33 PUBLICATIONS **44** CITATIONS
SEE PROFILE

Maha Abd Alellah
University of Mosul
10 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Journal of Engineering Science and Technology
Vol. 15, No. 6 (2020) 3639 - 3648

THE DETECT DOS ATTACK FROM NETWORK TRAFFIC USING GRAY WOLF OPTIMIZATION ALGORITHM

MUNA M. T. JAWHAR[1,*], MAHA A. ALELLAH[2]

[1]Software Engineering, Computer and Mathematical science, University of Mosul, Mosul, Iraq
[2]Software Engineering, Computer and Mathematical science, University of Mosul, Mosul, Iraq
*Corresponding Author: dr.muna_taher@uomosul.edu.iq

Abstract

A DoS attack can temporarily suspend the service or damage the system itself by consuming all system platforms such as memory, network bandwidth, CPU, etc., as seen in the incidents of commercial web servers. The damage can be extended to all network-related systems. Since this type of attack is dangerous to systems and networks, many researches are continuing to detect this type of attack and how to avoid the DoS attack. In this research a model for detecting DoS attack is presented. Intelligent techniques are used to minimize its damage. Specially swarm techniques, and more specially the gray wolf algorithm is used in detecting the attack. By taking the data from the packet of network and after analysing it, it is entered into the wolf algorithm, the results of the wolf algorithm were analysed and tested to obtain the attack detection rate with the false alarm and the negative alarm. The results were satisfactory and good. We used Matlab language version 10 on the Windows 10 operating system with the TCP/IP protocol.

Keywords: Denial of service attacks, Grey wolf optimization, Algorithm network security.

1. Introduction

A Denial of Service (DoS) attack is an attempt to make a machine or network resources unavailable for its intended users. Though the processes, motives, and targets of these attacks may vary, generally the intent is to interrupt or suspend services of a host (for example a web server) on the Internet. DoS attacks cause service server disruption by draining victim resources to render it unable to respond to the legitimate user [1]. Once the attack was identified, they will able to resolve this instance.

Optimization Issues are defined as a search process to determine the best solution for a particular issue. This search is done by agents according to certain rules of mathematical models, and these customers are constantly adapting to the best solution in the search space until a balance is reached where the search stops. Optimization issues are solved using optimization algorithms, often referred to as tools or techniques to solve optimization problems to find the best solution. The search for optimal solutions is complicated by the fact that real world problems are often associated with uncertainties. So real-life applications need solutions that are not only optimal, but are as robust as the solutions required in engineering and industrial designs [2].

There are two types of optimization techniques: the first type is Exact Strategies, which ensures the best solution that works well for many issues, but when it comes to complex issues or issues that contain a large number of parameters, these strategies may need to very high arithmetic costs. A large number of real-life issues fall into the category of complex issues to resolve in a reasonable amount of time. A different approach to this type of issue is needed. The second type is artificial intelligence techniques that are very efficient in finding the optimal solution [3]. One of this artificial intelligence is gray wolf algorithm.

The gray wolf algorithm was introduced by Mirjalili et al. in 2014 [4, 5]. This algorithm mimics the social leadership and behaviour of phishing gray wolves in nature. Where the division of society into four sections [6]:

α: denoted by Alpha symbol.
β: denoted by Beta symbol.
δ: denoted by Delta symbol.
ω: denoted by Omega symbol.

Gray wolves live in groups of group members with an average of 5 to 12 members. The commander is called Alpha, who is responsible for making decisions regarding fishing, sleeping, wake-up time, etc. These decisions are dictated to the rest of the group and the latter recognizes the leader's decisions by tail downwards. It is important to choose a leader and be Alpha for a group of individuals that is best at managing people and does not have to be strong in personnel management, which shows that good organization and good discipline among individuals is far more important than the power factor [7].

The last level in the sequence of personnel management in the group is Omega where it represents the lowest level in the group which must succumb to other dominant wolves. May appear insignificant but observed in the absence of Omega wolves arises an internal conflict in the group among high-level wolves where the Omega wolves maintain continuity of dominance [8]. The second level in gray wolves is a beta, a wolf attached to alpha that helps them make a decision. It

represents an alpha helper, a house wolf that respects an alpha wolf, but orders other lesser wolves. Beta wolf is the best candidate to be the leader in age or died.

If the wolf is not one of the three previous species it is a Delta type. Delta acquiesces to Alpha and Beta but dominates Omega. There are several types of Delta Wolf, such as the Scouts, Hunters, Group Guards, and Elders (Alpha and Beta Wolves). Figure 1 illustrates the hierarchy of hegemony from top to bottom in the gray wolf community [4].

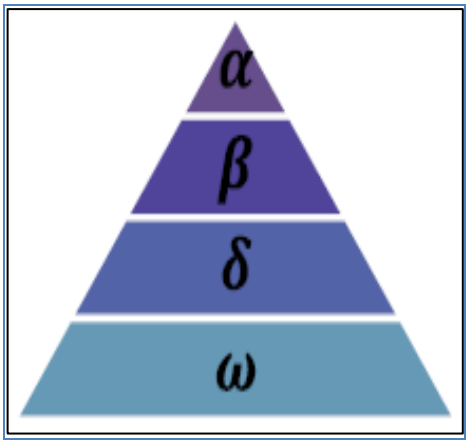

Fig. 1. Illustrates the hierarchy of hegemony.

This research is organized as following: Section 2, literature review, Section 3, Denial of Service, Section 4, Grey wolf optimization algorithm, Section 5, the proposed method, results and finally Section 6, the conclusions.

2. Literature Review

The researches in this area is rare. The following is mentioning most of them. Velliangiri et al. [9] research, used the Genetic algorithm with the gray wolf algorithm using the RBF function and LMS algorithm. They used genetic algorithm for adjusts the Weights of RBF neural and then used LMS algorithm. They used DARPA 99 Datasets for detect Dos attack.

Seth and Chandra [10] proposed a metaheuristic cloud detection system. The gray wolf algorithm has been modified to select the best features or attributes from the set of data entered into the system while k-NN is used for binary classification of inputs. The data used in this paper from TCP dump data.

Yang and Zhou [11] designed an intrusion detection system optimized by a cloud grey wolf (CGWO) algorithm.

Srivastava1 et al. [12] used improved gray wolf algorithm to detect network attacks with KDD-dataset. Data features were reduced from 41 to 24 features using three different techniques: "K-nearest neighbour (KNN), support vector machine (SVM) and Generalized regression neural network (GRNN) to classify the data into normal or attack class".

3. Denial of Service (DoS)

This type of attack prevents the legitimate user from enjoying internet services. Examples of this type of attacks: Attempts to flood the network with unnecessary packets and thus prevents the user from accessing the services. It tries to disconnect between two devices and thus prevents the service, and Attempts to prevent legitimate users from accessing the service provider in any way.

The attacker carefully studies the network's methodology and look for weaknesses and bottlenecks in the network and have access to all the devices connected to the network to be able to disconnect the service. Because the attacker did not participate in the attacks, making the process of tracking and detecting its source difficult and complicated. Known examples of such attacks are "Smurf, SYN Flood, and User Datagram Protocol (UDP) Flood" [13, 14].

4. Grey Wolf Optimizer (GWO)

As a mathematical model of algorithm is approach which simulate the grey wolves' leadership and hunting in nature. These approaches present one of the most important artificial intelligence algorithms by simple concepts [15].

The mathematical model of the encircling behaviour is represented by Eqs. (1) and (2):

$$z = \left|hy_{p(n)} - y(n)\right| \tag{1}$$

$$y(n+1) = y_{p(n)} - qz \tag{2}$$

where *z* represents the distance between the prey and the wolf, y_p represents the prey site, $y(n)$ represent the gray wolf site in the current session, $y(n+1)$ represent the gray wolf location in the new session, The vectors q and h are calculated using Eqs. (3) to (5) [16].

$$q = 2ir1 - i \tag{3}$$

$$h = 2r2 \tag{4}$$

$$i\text{=2-cycle(2 / MCN)} \tag{5}$$

where cycle indicates number of courses and MCN indicates number of total courses. i decreases linearly from 2 to 0 during the course, r1 and r2 are vectors range from 0 to 1.

In the abstract search space there is no idea of the location of the optimal solution (the prey site for the algorithm), In order to simulate the hunting behaviours of gray wolves mathematically, alpha, beta and delta wolves are presumed to have the best knowledge of the potential location of the prey, So the sites of these wolves are the best solutions. The alpha wolf has a higher priority followed by beta then delta [9]. This forces the rest of the wolves to update their location according to the location of the best wolf as in Eqs. (6) to (13) [17]:

$$z_\alpha = |h1\, y_\alpha - y| \tag{6}$$

$$z_\beta = \left|h2y_\beta - y\right| \tag{7}$$

$$z_\delta = |h3y_\delta - y| \tag{8}$$

$$y1 = y_\alpha - q1z_\alpha \tag{9}$$

$$y2 = y_\beta - q2z_\beta \tag{10}$$

$$y3 = y_\delta - q3z_\delta \quad (11)$$

$$y(n+1) = \frac{y1+y2+y3}{3} \quad (12)$$

$$Cycle=cycle+1 \quad (13)$$

where z_α , z_β , z_δ the vector location of the prey is represented by wolves α , β , δ ., $y1$, $y2$, $y3$ represent the modern sites of wolves α , β and δ, y is the vector represents the location of the current gray wolf, $y(n+1)$ is the vector of the new gray wolf site (updated) [17, 18].

In order to find good and preferred solutions in the algorithm, the wolves must separate from each other and then meet when the best solutions where the wolf Alpha has the highest preference followed by the wolf beta and then the wolf delta. The rest of the wolves are forced to update their location according to the location of the best wolf, and Fig. 2 Gray and its likely next location [19].

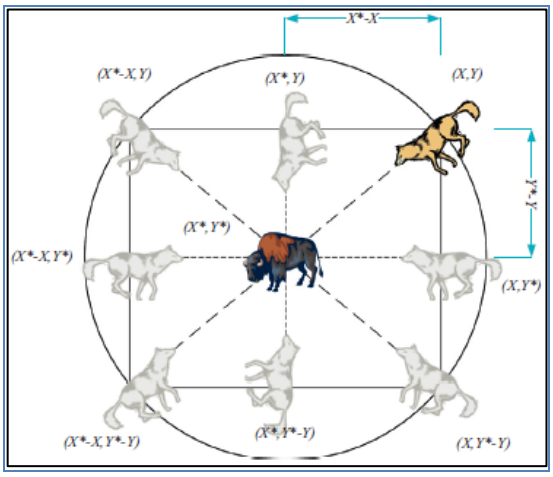

Fig. 2. The location of the gray wolf and its likely next location.

5. Experiments and Results

In practice, there is no intrusion detection system that ensures 100% detection of attacks or breaches. In this research, the proposed method for the detection of parasitism using a gray wolf intelligence algorithms.

The intelligence algorithms of the squadron of algorithms that mimic the social behaviour of the herds, herds and the schools of creatures in nature, the principle of its work that the group of customers continue and move through the search space according to certain rules using the simulations of social and social intelligence of creatures and the most famous of these algorithm gray wolf optimization algorithm (GWO).

The general structure of the method used in this research is to take the data packet from offline network traffic, analysed and configured to enter it into the wolf algorithm and then processing the results to reveal this package whether it was a type of attack or was normal as illustrated in Fig. 3.

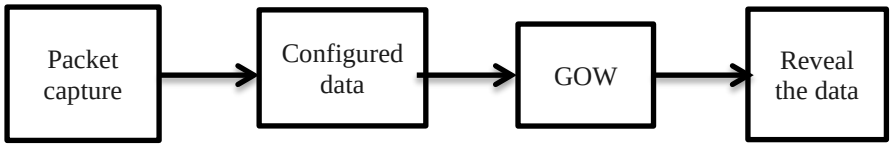

Fig. 3. The block diagram of the model.

The gray wolf optimization algorithm was used in this search, where data was taken from the previous step, where the work begins with the creation of a random community of gray wolves (candidate solutions) in the algorithm, and the research depends on the optimal solution through the best locations for wolves' alpha, beta and delta.

The goal function was defined as the fitness function where the highest values (max. value) were adopted to reach the best solutions. The total number of courses was determined by five courses. In the research, the value of MCN = 5 was adopted, and the values of i were linearly reduced from 2 to 0. Figure 4 is describing GWO flowchart

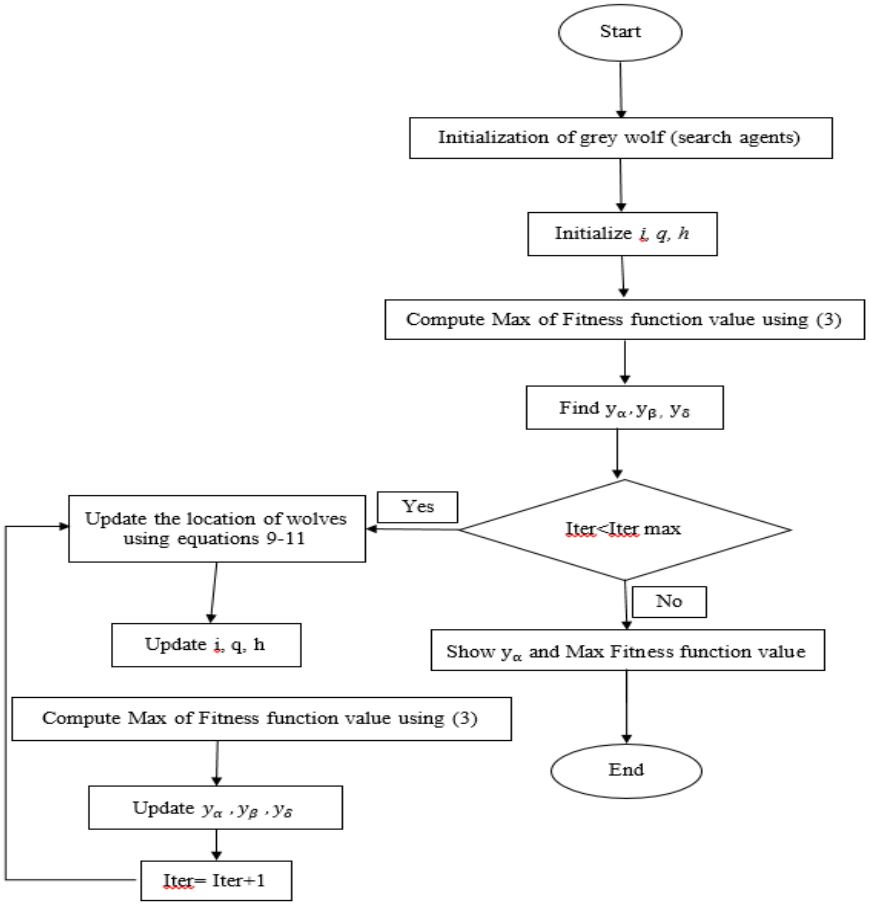

Fig. 4. The framework of the GWO algorithm.

As long as the cycle criterion is less than the number of cycles, the equation is performed from Eqs. (6) to (12). Then the values of *q, c, i* are updated and then the

target function for each element is updated and values are updated y_α , y_β ,y_δ Then the cycle value is updated according to Eq. (13) and the stop criterion is checked.

In order to find good and distinctive solutions in the algorithm, the flock of wolves must separate from one another then meet when the best solutions where the wolf Alpha has the highest preference followed by the wolf beta and then the wolf delta.

The values that resulted from the algorithm are alpha, beta, and delta, the average was taken for these three values and the largest value (maximum- max) with the smallest value (minimum- min) was tested with the real values and the results were as follows:

When testing the rate, the result was 70.79% the correct detection ratio. However, when testing for the smallest value, the ratio was 86.72% while the result of tested highest value was 93.80%. When testing the alpha value, the ratio was 82.30%.

The specific terms used in the classification of attacks used by all researchers in this field is true positive (TP), false negative (FN), false positive (FP) and true negative (TN).

One of the most important measures used in detecting attacks is accuracy and false alarm. Accuracy is defined as correct prediction, while false alarm is correct or natural restrictions are classified as an attack as show in Eqs. (14) and (15):

Accuracy = (TP+TN)/(TP+FP+FN+TN) or all records (14)

False alarm= FP/(FP+TN) (15)

Table 1illustrates the measures used in the model:

Table 1. Explain the testing result of the model.

	Average	Min.	Max.	Alfa
False alarm (%)	68.08	0	0	90.62
Accuracy (%)	33.23	33.23	32.93	32.93
TN (%)	26.54	10.61	2.65	8.84

After several tests we noticed that using the value of the max gives the highest detection rate of attack from the rest of the selected values as recorded in Table 1.

Figures 5, 6, and 7 illustrate the resulted test of the model.

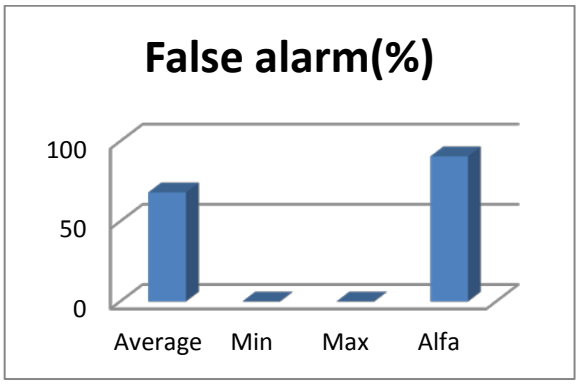

Fig. 5. The false alarm of the experiment.

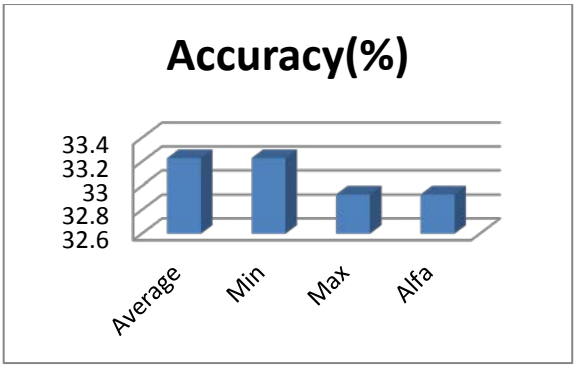

Fig. 6. The accuracy of the experiment.

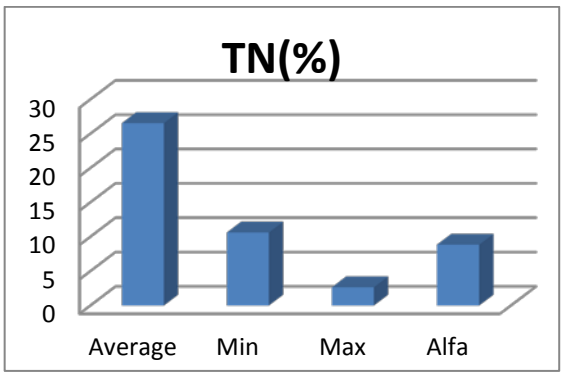

Fig. 7. The true negative of the experiment.

The results obtained from the model were compared with the results of previous research as shown in Table 2.

Table. 2. Comparison of the results with other researches.

Technical	Accuracy (%)
Our-GWO	32.93
GWO-KNN	77.9
GWO-SVM	79.5
GWO-GRNN	75

6. Conclusion

Because of the importance of the subject of networks and communications and the Internet services of large and wide user, so it is necessary to maintain the security of networks and the confidentiality of private data from various attacks and intruders who try to steal and block the user's work. So, we note many of the research addressed to the subject of maintaining data security and detecting and responding to attacks. So, we had a share in the study of the attack and how to detect it using the wolves' algorithm and the results after many experiments were fairly good.

The intelligence of the swarms is a distributed smart model for the purpose of solving optimization problems. One of the most popular intelligence algorithms used

in this research is the gray wolf optimization algorithm, which is concerned with the intelligent system inspired by the behaviour of the gray wolf in the search for prey. The most important characteristic of gray wolf optimization is that it highly experienced in modified and tested on Dos attack detection.

Algorithm has been able to give positive feedback on the data that has been introduced for quick exploration of good solutions. Where the algorithm helped to flexibility and adaptation in dealing with data in the case of failure of one of the wolves, they continue to complete the task in addition to the possibilities of self-regulation and efficiency in solving optimization issues.

References

1. Seo, J.; Lee, C; and Moon, J. (2004). Defending DDoS attacks using network traffic analysis and probabilistic packet drop. *International Conference on Grid and Cooperative Computing*, Springer-Verlag Berlin Heidelberg, German, 390-397.
2. Gholizadeh, S. (2015). Optimal design of double layer grids considering nonlinear behaviour by sequential grey wolf algorithm. *Journal of Optimization in Civil Engineering*, 5(4), 511-523.
3. Mittal N.; Singh U.; and Sohi B.S. (2016). Modified grey wolf optimizer for global engineering optimization. *Applied Computational Intelligence and Soft Computing*, 2016, 1-16.
4. Mirjalili, S., Mirjalili, S.M., and Lewis, A. (2014). Grey wolf optimizer. *Advances in Engineering Software*, 69, 46-61.
5. Mirjalili, S. (2015). How effective is the grey wolf optimizer in training multi-layer perceptron. *Applied Intelligence*, 43, 150-161.
6. Naderizadeh, M.; and Baygi, S.J.M. (2015). Statcom with grey wolf optimizer algorithm based pi controller for a grid Connected wind energy system. *International Research Journal of Applied and Basic Sciences*, 9(8), 14-21.
7. Saremi, S.; Mirjalili, S.Z.; and Mirjalili, S.M. (2015). Evolutionary population dynamics and grey wolf optimizer. *Neural Computing and Applications*, 26(5), 1257-1263.
8. Sulaiman, M.H.; Mustaffa, Z.; Mohamed, M.R.; and Aliman, O. (2015). Using the grey wolf optimizer for solving optimal reactive power dispatch problem. *Applied Soft Computing*, 32, 286-292.
9. Velliangiri; Cristin, S.; and Karthikeyan, R. (2018). Genetic gray wolf improvement for distributed denial of service attacks in the cloud. *Journal of Computational and Theoretical Nanoscience*.15, 2330-2335.
10. Seth, J.K.; and Chandra, S. (2018). MIDS: Metaheuristic based intrusion detection system for cloud using k-NN and MGWO. *International Conference on Advances in Computing and Data Sciences*, Springer.
11. Yang, H.; and Zhou, Z,. (2018). A Novel intrusion detection scheme using cloud grey wolf optimizer. *37th Chinese Control Conference* (CCC), Wuhan, China.
12. Srivastava1, D.; Singh, R.; and Singh, V. (2019). An Intelligent gray wolf optimizer: A nature inspired technique in intrusion detection system (IDS). *Journal of Advancements in Robotics*, 6(1). 18-21
13. Lau, F.; Rubin, S.H.; Va, S.; Smith, M.H.; and Trajkovic, L. (2000). Distributed denial of service attacks. *Institute of Electrical and Engineers*, 3 (1).

14. David, R.; and Midkiff, S.F. (2008). Denial of services in wireless sensor. *Institute of Electrical and Engineers*, 7(1), 71-81.
15. Wong, L.I.; Sulaiman, M.H.; and Mohamed, M.R. (2015). Solving economic dispatch problems with practical constraints utilizing grey wolf optimizer. *Applied Mechanics and Materials*. Trans Tech Publications.
16. Yusof, Y.; and Mustaffa, Z. (2015). Time series forecasting of energy commodity using grey wolf optimizer. *Proceedings of the international multiconference of engineers and computer scientists*, Hong Kong, China.
17. Mirjalili, S.; Mirjalili, S.M.; and Lewis, A. (2014). Grey wolf optimizer. *Advances in Engineering Software*, 69, 46-61.
18. Pradhan, M.; Roy, P.K.; and Pal, T. (2016). Grey wolf optimization applied to economic load dispatch problems. *International Journal of Electrical Power and Energy Systems*, 83, 325-334.
19. Kumar, A.; Pant, S.; and Ram, M. (2017). System reliability optimization using gray wolf optimizer algorithm. *Quality and Reliability Engineering International*, 33(7), 1327-1335.