International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 27, No. 3, June, 2022, pp. 441-446
Journal homepage: http://iieta.org/journals/isi

Intrusion Detection Network Attacks Based on Whale Optimization Algorithm

Sundus Abdulmuttalib Mohamed[1,2*], Omar Ibrahim Alsaif[2], Ibrahim Ahmed Saleh[1]

[1] College of Computer Science and Mathematics, University of Mosul, Mosul 41001, Iraq
[2] Mosul Technical Institute, Northern Technical University, Mosul 41001, Iraq

Corresponding Author Email: sundus_abid7@uomosul.edu.iq

https://doi.org/10.18280/isi.270310

Received: 18 February 2022
Accepted: 7 June 2022

Keywords:
anomaly, intrusion detection, network attack, whale optimization algorithm

ABSTRACT

Network intrusion detection is a significant issue faced by the Information technology industry. Hacker's attacks set of techniques cause confusion network and computer systems, therefore, the need for a network penetration detection process became urgent. This paper proposed an optimization method to detect the potential of attacks on network packets effectively by defining unfamiliar patterns in a massive volume of the network traffic. Initially, the packet characteristics are defined as the normal dispersal of attributes from the data packet. This algorithm is used a bio-inspired meta-heuristic technique named whale optimization algorithm (WOA) to detect systems against the attackers. The detection method whale optimization (DMWO) is applied to calculate the process of standard deviation distribution to judge the anomaly of the data packet. The simulation algorithm performed by OPNET and Matlab-2015a to main factors of DMGO to classify the input to check whether any attack is present or not. Finally, the performance of this algorithm is a better flexibility result compared with other algorithms DMCM and IHMM.

1. INTRODUCTION

Intrusion detection systems (IDS) are designed to observe all events in computer and determine some observed traffic data is normal or abnormal. IDS is used to trace any suspicious activity from an attacker and help computer systems how to deal with attacks and prepare to them [1, 2]. Network attacks have brought great security risks to users that appeared with the rapid development of the internet as well as the unauthorized access. The effective detection and defense attacks have become a challenge and hotter topic from focus topic of researcher's interest [3-6]. Currently, attack events can be divided into four categories based on attack determined: Denial of service attacks (DoS), Remote to local attacks (R2L), User to root attacks (U2R), and Probes. The DoS type destroys the effectiveness of network services, making the host or network unable to receive and process external requests on time, thus cannot provide normal services to legitimate users. The detection methods of network attacks can be divided into:

1) Hidden Markov model: each attack intention through an algorithm that calculates probability to each state to identify normal and abnormal traffic during testing.

2) Bayesian rules: is based on learning the behavior of the model and predicts the probability of attackers and provides protection that will be selected against the attacker for the next phase of the system.

3) Colored timed Petri nets focus on detecting attack events by attached data value.

4) Correlation of attack response events implement analyzing the context of the attack, and predict the possible attack probability of the same attacker on the same object.

Due to the real traffic has fractal and burst features, the fractional statistical model of network detection called "Autoregressive IntegratedMoving Average ARIMA (p, d, q)" that better describe the characteristics of the traffic fractal and burst [7, 8], therefore it can be combined with the model to arrive. This model can be used to fit the packet to packet that analyzes the abnormality of network traffic.

Moreover, the contribution proposed to be as follow:

- Intrusion detection for network attacks;
- Apply meta-heuristic algorithm whale optimization algorithm (WOA) detects systems against the attackers;
- Modify new algorithm called DMWO to calculate the process of standard deviation distribution to judge anomaly of the data packet.

The proposed method gives the detection index based on the dispersion of the packet attributes, and judges the existence of the packet by obtaining the standard deviation distribution of the packet attributes Likelihood of being attacked. We simulate our propose algorithm using OPNET and MATLAB to carry out comparison experiments by comparing the performance of this algorithm with other algorithms DMCM and IHMM.

The structure of the paper is as follows: Section2 related works; Section3 illustrate cyber-attack evaluation index which happen from one or more computers; Section4 establishes an attack detection method combined with a whale optimization algorithm; Section5 performs simulation experiments on the detection algorithm. Finally Section 6 illustrated conclusion of the paper.

2. RELATED WORKS

In this paper, many researchers have explored a lot of work for intrusion detection. Ngai et al. [9] have propose intrusion detection that used multiple attributes of node behavior characteristics. The authors combined with accurate detection of attack behavior and to effective fusion of sensor data, to establish an efficient network attack detection method. In order to reduce the network overhead as well as the false alarm rate; The authors obtain the real-time status information of both the client and the server using a lightweight protocol interaction method. While Mean Daniyar [10] used the Firefly Harmonic Clustering Algorithm (FHCA) model to describe the abnormal behavior of the data packet. The algorithm is an established method for detecting abnormal traffic state of the disaster progression; the false alarm rate of attack detection required to improve. Consequently, Hoque et al. [11] introduce a genetic algorithm for the intrusion detection system. The authors applied information theory on KDD99 benchmark dataset to volute the filter the traffic data and reduce the complexity. Mangrulkar et al. [12], combined four different detection methods used Hidden Markov with distributed denial of service (DDoS) attacks. This model only used for network layer protocols and there is no effective detection mechanism for the application layer. Cusack and Almutairi [13] established an adaptive security framework against DoS attacks in peer-to-peer networks.

While, Chen et al. [14] proposed the principle to determine the behavior of the natural text samples. The improved hidden Markov model is used to establish a network intrusion detection which aiming to monitor characteristics of abnormal network behavior that deviates from regular grammar rules. Finally, Zhou et al. [15] introduce a heuristic algorithm called "Correlation-based Feature-Selection-Bat-Algorithm" (CFS-BA) to intrusion detection for network traffic, which used feature selection with KDDCup99 dataset to train and test attributes of packets and detected which one is lowest False Alarm. paper Inthis we propose the detection method whale optimization (DMWO) which applied to calculate the process of standard deviation distribution to judge the anomaly of the data packet. The simulation algorithm performed by OPNET and Matlab-2015a to main factors of DMGO to classify the input to check whether any attack is present or not.

3. CYBER-ATTACK EVALUATION INDEX

The Cyber-attacks are assaults launched organized by attackers from one or more computers against the information and telecommunications systems. Cyber-attacks aims to steal or damage the information of certain institutions and affect these institutions economically and or politically [16].

Since a data packet in HTTP protocol can be regarded as a string that follows a certain standard for a data field has k common attributes, the data packet represents as $Y=[y_1, y_2, ..., y_k]$, where y_k represents the data header, the Host header department, source IP address, destination IP address,…etc. For the sample set of n packets, it can be expressed as:

$Z=[y_{11}, y_{21}, \dots\ y_{1k}, y_{21}, y_{22}, \dots, y_{2k}.\ y_{n1}, y_{n2}, \dots, y_{nk}]$

$$Z = \begin{bmatrix} y_{11} & y_{21} & \cdots & y_{1k} \\ y_{21} & y_{22} & \cdots & y_{2k} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ y_{n1} & y_{n2} & \cdots & y_{nk} \end{bmatrix} \tag{1}$$

Then the kth is attribute of n packets can be represented by sequence $Z_k=[y_{1k}, y_{2k}, ..., y_{nk}]$. Assume the scuttle of kth attribute be $\beta(Zk)$, then the dispersion $\beta(Z)$ of entire sample set is [16]:

$$\beta(\mathrm{Z}) = 1/\mathrm{k} \sum\text{\_}(\mathrm{i} = 1)\text{\^{}}\mathrm{k}\ \beta(\mathrm{Z\_i}) \tag{2}$$

Assume the average dispersion of an attribute k is $\beta(Zk)$, the standard deviation λ is used here to describe deviation between packet attribute and overall average dispersion:

$$\lambda = \sqrt{\frac{1}{n}\sum_{i=1}^{k}(\beta(Z_i) - \beta\ (Z_k)} \tag{3}$$

Among them, the larger λ means that farther packet deviates from the standard sample more likely it is to be tampered with by attack. Due to indicators, we established a detection method based on the cloud model (DMCM).

In the cloud model:

- Data packet consider to be detect $Y=[y_1, y_2, …., y_k]$ as a cloud drop,
- Cloud group is composed of a series of cloud drops,
- The proposed cloud drop represents a realization of a qualitative object and the order between the cloud drops is irrelevant,
- Cloud drops are generated in the domain according to the defined rules. The generator generates random degree of certainty in the domain, and through this random degree of certainty. The subsequent cloud generator activates to generate new cloud droplets. However, due to the broad uncertainty of the cloud model. The amount of calculation is too large. Therefore, we use (WOA) to establish a new network attack detection method to reduce the amount of calculation whereas avoiding falling into local optimum.

4. RESEARCH METHODOLOGY

4.1 Whale optimization algorithm

The whale optimization algorithm simulated the intelligence hunting behavior of humpback whales. The behavior is called "bubble-net" that only humpback whales take when seeking their food. The whales make typical bubbles along a circular path whereas encircling prey during hunting. The whales enclose prey by making classical bubbles along a circle path then create the bubble in a spiral shape around the prey later swim up the surface following the bubbles as shown in Figure 1 [17, 18].

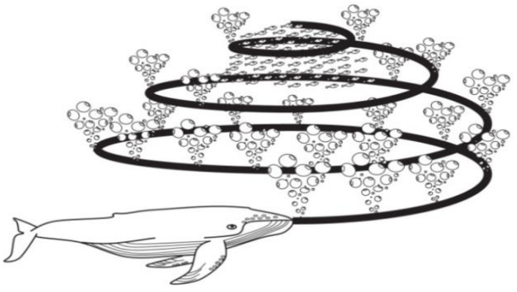

Figure 1. Bubble-net of humpback whales

The WOA considers the current best search agent position to be the target prey or near the optimum point, meanwhile other search agents will try to update their position towards the best search agent. The behavior formulates as the following equations:

$$D^{\rightarrow} = |C^{\rightarrow}.(X^{\wedge} *)^{\rightarrow}(t) - X^{\rightarrow}(t)| \tag{4}$$

$$X^{\rightarrow}(t + 1) = (X^{\wedge} *)^{\rightarrow}(t) - A^{\rightarrow}.D^{\rightarrow} \tag{5}$$

where, *t* is current iteration, *X** indicates to position vector of the best solution, and *X* represent the position vector for each agent. The coefficient vectors $A^{\rightarrow}$ and *C* are calculated as follows:

$$A^{\rightarrow} = 2\,a^{\rightarrow}.r - a^{\rightarrow} \tag{6}$$

$$C^{\rightarrow} = 2r \tag{7}$$

where, $a^{\rightarrow}$ is linearly decreased from 2 to 0 over the iteration path and r random number with a period between [0, 1]. Variable is had decreasing value to accomplish the contraction encircling mechanism of bubble-net attacking technique. To spiral updating position is a spiral equation is created between the whale position and victim to simulate movement of whales as follows [18, 19]:

$$D^{\rightarrow} = |(X^{\wedge} *)^{\rightarrow}(t) - X^{\rightarrow}(t)| \tag{8}$$

$$X^{\rightarrow}(t + 1) = (D^{\wedge\prime})^{\rightarrow}.e^{\wedge}bl\,cos\,cos\,(2\pi l) + (X^{\wedge} *)^{\rightarrow}(t) \tag{9}$$

where, $D^{\rightarrow}$ is the distance between whale and victim, b is constant defines the logarithmicshapeisrandomin [−1, 1].

In Search stage in the algorithm, the whale explores using random selection for the optimum prey. In contrast to the exploitation stage, in this phase consider, $A^{\rightarrow}$ the vector to be a random value more than 1 or less than −1. With this assumption, the search agent can move far from a reference whale. In return, the position of the search agent will be updated according to the randomly chosen search agent, instead of the best search agent found so far. These two actions formulated as follows:

$$D^{\rightarrow} = |C^{\rightarrow}.(X\_rand)^{\rightarrow} - X^{\rightarrow}| \tag{10}$$

$$\mathrm{X}^{\rightarrow}(\mathrm{t} + 1) = (\mathrm{X\_rand})^{\rightarrow} - \mathrm{A}^{\rightarrow}.\mathrm{D}^{\rightarrow} \tag{11}$$

where, X_{rand} is a random position vector WOA algorithm is a global optimizer; the algorithm starts from a set of random solutions. At each iteration, search agents update their position according to the above constructions. Adaptive variation of the search vector $A^{\rightarrow}$ allows to algorithm transit between exploration and exploitation. Moreover, High exploration ability of WOA is updating mechanism of position of whales using (11). High exploitation and convergence asserted, which originate from (9) and (5). These equations show that the WOA algorithm can provide high local optima avoidance and speed convergence during the iteration [20, 21].

4.2 Intrusion detection with WOA

In order design a force system that keeps the security of the computer network and enhances the resistance to external intrusion. It is necessary to create a perfect security protection system to carry detection and protection of network, the system is used WOA based on DMCM to perform these two processes. However, whale optimization algorithms easily lead to local optimization, so this paper combines mutation operators to improve the shortcomings of WOA algorithms to improve the success rate of detecting network attacks. The specific algorithm DMWO is as follows [22]:

1) Initializing the network parameters at the determining the whales size n, generating=30, lb=-100; ub=100; dim=30;

2) Considering a data packet *Y*=[y_1, y_2, ..., y_k] to be detected as the whale. The whale is resolving whether the standard deviation λ of current agent i is smaller than the threshold λ max or not.

- if not satisfied according to Eqns. (8) and (9) there are different values equal to about 50% for whales' behavior.

- Else if whale choosing either the shrinking encircling movement or the spiral model movement is simulated during iterations of the algorithm. It means that:

$$\begin{aligned}\vec{X}(t+1) = \{\overrightarrow{X^*}\,(t) - \vec{A}.\vec{D}\; if\; p \\ < 0.5\,\overrightarrow{D'}.e^{bl}\,cos\,cos\,(2\pi l) \\ +\;\overrightarrow{X^*}\,(t)\; if\; p \geq 0.5\end{aligned} \tag{12}$$

where, *p* is random number in [0, 1].

3) Calculate the fitness value *f*(*λ*) of whale agent according to the fitness function shown in (13) [23]:

$$f(\lambda) = 1/(1 + e^{\wedge}(-\lambda)) \tag{13}$$

Then determining the optimal position spot of the whale as the current position, and temporarily making the spot the optimal position s of a current best agent.

4) Spiral update position between whale and victim according to the current optimal position spot, combined with Eqns. (9) and (8).

5) If the standard deviation λ of thew hale is less than threshold λ max, jump to step (6), otherwise uses D as the initial point and replace X(t+1) illustrated in Eqns. (10) and (11) with recalculating its fitness;

6) Determine whether the fitness of humpback whales is better than the fitness of X(t) and if so, let X(t+) be the fitness value.

7) Output the standard deviation λ(i) of the current particle, and let i=i+1, jump to step (2) and repeat the calculation until all the standard deviation distributions of the λ=[λ(1), λ(2), ..., λ(k)] whereas judging whether each λ(i) exceeds a prescribed threshold, and if it is exceeded, there is a possibility of being attacked;

8) The algorithm ends [24].

5. SIMULATION EXPERIMENTS

Aiming at the above improved DMWO algorithm, this paper uses OPNET and Matlab2015a to achieve simulation experiments to verify its effectiveness. The simulation topology (shown in Figure 2) is established based on OPNET. There are (5 PC-nodes) in the left side (A) and (S) nodes whereas on the right side (F, G, D) ,the node_S is a data source that sends a packet to node_D (destination node) ,the node_F is an attacker.

Assuming the network parameters as follows:

- Each data packet size is 512b; the link bandwidth is 20M.
- Each network node buffer is 1024Kb, and the delay is10ms.
- Node_S is the data source (IP address 192.168.1.1).
- Node_D is data receiver (IP address 192.168.1.100).

- Node_F is the attack source (IP address 192.168.1.2).

- Regular attacks are launched into the network (including DoS, Probe, R2L, U2R, etc.).

- The rest are transit nodes (the IP addresses from node A to node G are 192.168.1.3 to 192.168.1.9 respectively).

- Set the agent whale n = 30, the variation distribution index φ=0.5, and the state up date parameter η=2.

Let node_S send 1000 packets per second to node_D, each packet Y=[y_1, y_2, y_3], y_1 represents the packet length, y_2 represents the packet timestamp, and y_3 represents the source end address of the packet. Set up monitoring at node_D, collect data packets sent from node_S, and perform state analysis to make node_F launch a DoS attack.

To further work, the performance of the DMWO algorithm. Suppose that node_F still launches a DoS attack.

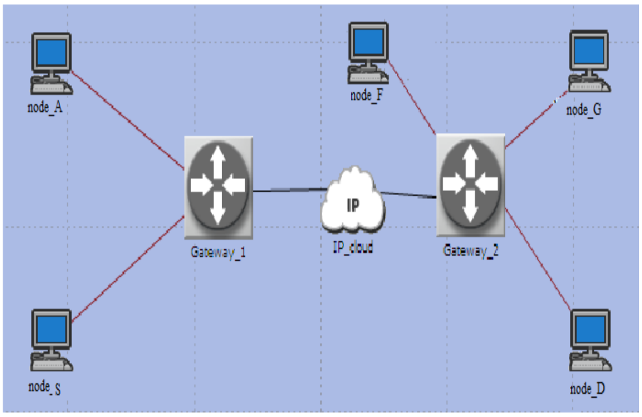

Figure 2. Proposed network

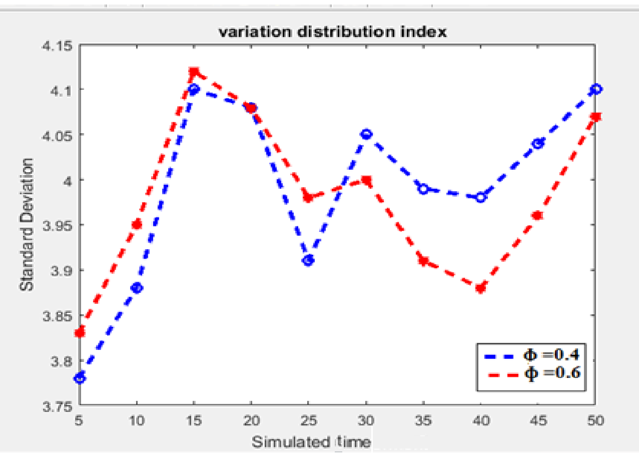

Figure 3. Different variation distribution index φ Comparison of standard deviation of packet length

Figure 3 shows a variation of the standard deviation λ of the packet length at different variation distribution indices φ. It can be seen that the beginning of the simulation show difference in distribution index. The smaller φ leads that the curve is smaller of standard deviation, and the larger variation distribution index φ have small value of the standard deviation for the curve. Because there are few data packets gathered at node_D in the previous period, the number of whale agents with a standard deviation λ smaller than the threshold λmax is smaller.

It can be seen in Figure 3 illustrated DMWO detection of packet length state (y1) in the node_D, that a smaller variation distribution index φ can obtain best position s (i, 0) and better of adaptive value f (λ), so that is smaller standard deviation λ of packet length. Also, the number of packets gathered at node_D increases the number of whale agents with a standard deviation λ smaller than the threshold λmax. The more variation distribution index φ is required to obtain the optimal position s (i, 0) and better fitness value f (λ), the more variation distribution index φ, the smaller the standard deviation of the curve.

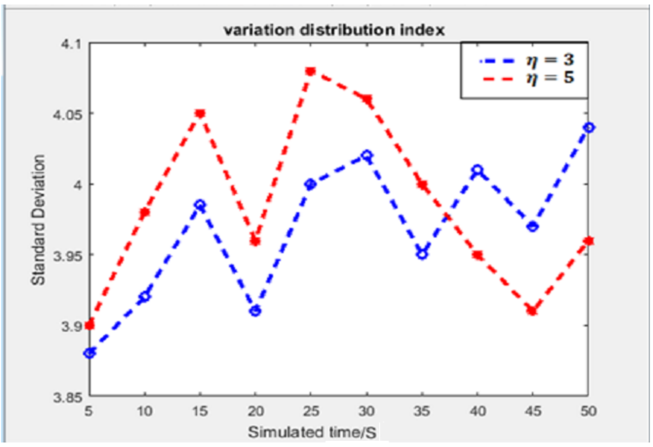

Figure 4. Compression of standard deviation of packet length under Different state update parameters η

In Figure 4 shows the standard deviation variation λ of packet length under different state update parameters η. Similar to the phenomenon in Figure 3, the curve suddenly changed. The update parameter state η in the initial simulation leads to a lower standard deviation of the corresponding curve, with larger state update parameter η in the later simulation leads to a lower standard deviation of the corresponding this curve. The reason is that in the initial simulation, there are fewer aggregated data packets at node_D, and the overall performance of the agent is low. A slight adjustment of the state update parameter η will have an accessible effect on the position of the agent, so it is easier to obtain a global optimum.

At this time, the larger the state update parameter η will increase the system overhead, which is not conducive to the global optimization operation. In the later simulation, with the increase of aggregated data packets and the improvement of the overall performance of the whale optimization, if we want to improve the performance of WOA, we need a relatively large state update parameter η, at this time, the large the state update parameter η, the smaller the standard deviation of the corresponding curve.

Data analysis performed on the inspection data compares among DMWO, DMCM, and IHMM (Improved HMM model-based method for detecting attacks) algorithm proposed in [9] and the actual monitoring results at node_D. The error between DMWO, DMCM, IHMM, and the actual results were: 3.62%, 5.05%, and 8.28% respectively.

It is clear from Figure 4 that after the experiment enters the stationary process (after 15s of simulation time), the standard deviation of the curve corresponding to DMWO is smaller than the other two algorithms. And from the perspective of the classical deviation jitter, DMWO also tends to be stable, whereas the IHMM corresponding curve has higher jitter.

In Figure 5 noticed the relationship between the standard deviation λ of the packet length and the initial position of the agent whale. It can be seen that when the initial position increments, the standard deviation shows a trend of decreasing first and then increasing. It is easy to understand. In the initial stage, the overall performance of the WOA is low. At this time, increasing the initial distance of the whale is conducive to faster convergence and global optimization. At this time, the standard deviation shows a downward trend; but after reaching the extreme value, the overall performance of the WOA is at a better level. Further, decrease the distance can only increase the system overhead and cannot achieve the purpose of improving performance, so the standard deviation shows an increasing trend, Table 1 shows the comparison of the detection success rate, false-negative rate, and false-positive rate of DMWO, DMCM, and IHMM algorithms when node_F launches DoS, Probe, R2L, and U2R attacks, respectively. As can be seen from Table 1, the performance of the improved DMWO algorithm has been significantly improved compared to DMCM and IHMM algorithms. The result of success rate better values compared to DMCM and IHMM algorithms Also the false positive in R2L is less values than others, therefore that DMWO has better adaptation.

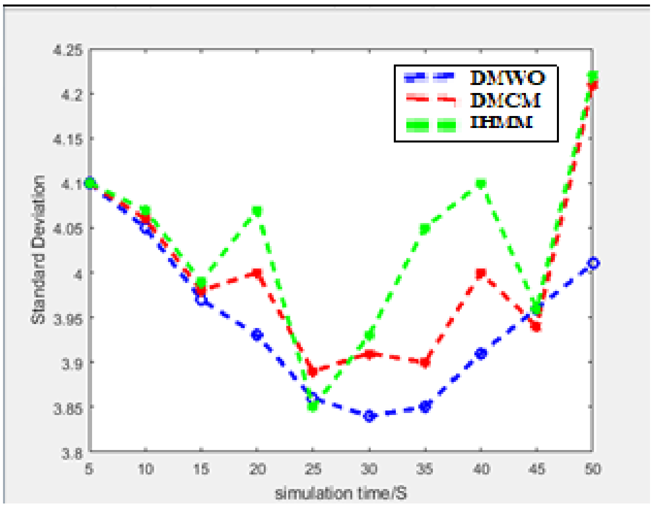

Figure 5. Comparisons of standard deviation λ

Table 1. Compression of test results under different attack types

Scales	Type of Attack	Dos	Probe	R2L	U2R
DMWO (%)	**Success Rate**	96.24	92.16	89.03	83.61
	Under reporting	3.77	8.75	8.01	15.83
	False Positive	0	0	2.99	0
DMCM (%)	**Success Rate**	94.29	89.88	87.15	82.89
	Under Reporting	4.43	10.79	9.75	17.31
	False Positive	0	0	3.72	0
IHMM (%)	**Success Rate**	92.85	87.13	84.28	80.72
	Under Reporting	8.85	13.59	11.29	19.88
	False Positive	0	0	6.34	0

6. CONCLUSIONS

To detect whether the network is affected by the attack or not, this paper proposes a new experimental result of network intrusion detection algorithm based on Whale Optimization DMWO. That demonstrated of facilitating simulated by OPNET-14 and Matlab 2015a, the algorithm defines packet sample discriminant index based on dispersion, and standard deviation of attributes of the packet that given 3.84, while IHMM and DMCM is given (3.86,4.1) respectively, the performance of DMWO, DMCM, and IHMM algorithms under different attack types compared. The results shows that DMWO has better adaptability, for different cases that discussed.

REFERENCES

[1] Kannan, A., Maguire Jr, G.Q., Sharma, A., Schoo, P. (2012). Genetic algorithm based feature selection algorithm for effective intrusion detection in cloud networks. In 2012 IEEE 12th International Conference on Data Mining Workshops, Brussels, Belgium, pp. 416-423. https://doi.org/10.1109/ICDMW.2012.56

[2] Selamat, S.R., Sahib, S., Hafeizah, N., Yusof, R., Abdollah, M.F. (2013). A forensic traceability index in digital forensic investigation. Journal of Information Security, 4(1): 27549. https://doi.org/10.4236/jis.2013.41004

[3] Ahmed, U., Raza, I., Hussain, S. A., Ali, A., Iqbal, M., Wang, X. (2015). Modelling cyber security for software-defined networks those grow strong when exposed to threats. Journal of Reliable Intelligent Environments, 1(2): 123-146. https://doi.org/10.1007/s40860-015-0008-0

[4] Yakobu, D., Kalluri, H.K., Dondeti, V. (2019). An enhanced secure, robust and efficient crypto scheme for ensuring data privacy in public cloud using obfuscation & encryption. Ingénierie des Systèmes d'Information, 24(6): 603-609. https://doi.org/10.18280/isi.240607

[5] Sharafaldin, I., Lashkari, A.H., Ghorbani, A.A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pp. 108-116. https://doi.org/10.5220/0006639801080116

[6] Zegeye, W.K., Moazzami, F., Richard Dean, R.A. (2018). Design of intrusion detection system (IDS) using hidden markov model (HMM). In Proceedings of the International Telemetering Conference, Glendale, AZ, USA, pp. 5-8.

[7] Vanitha, L., Mary, M.S. (2016). A comparative study of Classification algorithms used in Network Intrusion Detection Systems (NIDS). ARS-Journal of Applied Research and Social Sciences, 3(23): 7-14.

[8] Harmantzis, F.C. (2005). Heavy network traffic modeling and simulation using stable FARIMA processes. In Proceedings of the 19th International Teletraffic Congress (ITC19).

[9] Zhou, B., He, D., Sun, Z., Ng, W.H. (2005). Network traffic modeling and prediction with ARIMA/GARCH. In Proc. of HET-NETs Conference, pp. 1-10.

[10] Ngai, E.C., Liu, J., Lyu, M.R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer Communications, 30(11-12): 2353-2364. https://doi.org/10.1016/j.comcom.2007.04.025

[11] Saleh, I.A., Alsaif, O.I., Yahya, M.A. (2020). Optimal distributed decision in wireless sensor network using gray wolf optimization. IAES International Journal of Artificial Intelligence, 9(4): 646-654. http://doi.org/10.11591/ijai.v9.i4.pp646-654

[12] Adaniya, M.H., Lima, M.F., Sampaio, L.D., Abrão, T., Proença, M.L. (2011). Anomaly detection using firefly harmonic clustering algorithm. In Proceedings of the International Conference on Data Communication Networking and Optical Communication System (DCNET-2011), pp. 63-68. http://doi.org/10.5220/0003525800630068

[13] Hoque, M.S., Mukit, M., Bikas, A.N. (2012). An implementation of intrusion detection system using genetic algorithm. International Journal of Network Security & Its Applications (IJNSA), 4(2): 109-120. http://doi.org/10.5121/ijnsa.2012.4208

[14] Mangrulkar, N.S., Patil, A.R.B., Pande, A.S. (2014). Network attacks and their detection mechanisms: A review. International Journal of Computer Applications 90(9): 36-39. http://dx.doi.org/10.5120/15606-3154

[15] Saleh, I.A., Alawsi, W.A., Alsaif, O.I., Alsaif, K. (2020). A prediction of grain yield based on hybrid intelligent algorithm. Journal of Physics: Conference Series, 1591(1): 012027. https://doi.org/10.1088/1742-6596/1591/1/012027

[16] Cusack, B., Almutairi, S. (2014). Listening to botnet communication channels to protect information systems. In Proceedings of the 12Australian Digital Forensics Conference, Held on the 1-3 December, Joondalup, Australia, pp. 44-52. https://doi.org/10.4225/75/57b3df16fb87b

[17] Chen, C.M., Guan, D.J., Huang, Y.Z., Ou, Y.H. (2016). Anomaly network intrusion detection using hidden Markov model. International Journal of Innovative Computing, Information and Control ICIC International, 12(2): 569-580.

[18] Zhou, Y., Cheng, G., Jiang, S., Dai, M. (2020). Building an efficient intrusion detection system based on feature selection and ensemble classifier. Journal of Elsevier, 174: 107247. https://doi.org/10.1016/j.comnet.2020.107247

[19] Starr, S., Kuehl, D., Pudas, T. (2010). Perspectives on building a cyber force structure. In Proc. Conf. on Cyber Conflict, pp. 163-181.

[20] Nasiri, J., Khiyabani, F.M. (2018). A whale optimization algorithm (WOA) approach for clustering. Cogent Mathematics & Statistics, 5(1): 1483565. https://doi.org/10.1080/25742558.2018.1483565

[21] Malathi, N., Devarajan, N. (2019). Whale optimization algorithm with constriction factor and amplitude matching technology for real time lower order modeling. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(6S): 249-257.

[22] Mirjalili, S., Lewis, A. (2016). The whale optimization algorithm. Advances in Engineering Software, 95: 51-67. https://doi.org/10.1016/j.advengsoft.2016.01.008

[23] Ning, G.Y., Cao, D.Q. (2021). Improved whale optimization algorithm for solving constrained optimization problems. Hindawi Discrete Dynamics in Nature and Society, 2021: 8832251. https://doi.org/10.1155/2021/8832251

[24] Madhu, S., Midde, R.R., Ramu, G., Jayanthi, A., Somasekar, J., Ramesh, G., Reddy, P.D.K. (2019). A secured framework to protect association rules in the big data environment using fuzzy logic. Ingénierie des Systèmes d'Information, 24(5): 531-537. https://doi.org/10.18280/isi.240511