China Petroleum Processing and Petrochemical Technology

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

SECURING THE DIGITAL REALM: UNLEASHING HYBRID OPTIMIZATION FOR DEEP NEURAL NETWORK INTRUSION DETECTION

[1]Thupakula Bhaskar, [2]B. J. Dange, [3]S. N. Gunjal, [4]H. E. Khodke

Corresponding Author Email: bhaskarcomp@sanjivani.org.in

[1,2,3,4] Sanjivani College of Engineering (Autonomous),

Kopargaon, Maharashtra, India

***Abstract*:** Businesses now care deeply about securing their data and warding off malware attacks with sophisticated and reliable solutions. There are a number of different algorithms used in the intrusion detection system (IDS), each with its own set of advantages and disadvantages. In this paper, we offer another way to deal with interruption discovery that joins Gravity search calculation with dark wolf streamlining (GSGW) and other half and half enhancement draws near. The dark wolf approach is a sort of assault identification and counteraction with a low misleading problem rate and a high location rate in light of the fact that to its leaderless design and steady watchfulness. Performance is evaluated through feature selection in the NSL-KDD dataset. Exploratory results show that the suggested strategy has a lower misdirection rate, higher precision, and better discovery contrasted with the benchmark.

Keywords: *IDS, Gravity search Grey wolf optimisation (GSGW), FAR (False Alarm Rate), DR (Detection Rate), and DR (Detection Rate)*

INTRODUCTION

Internet connectivity is now essential for the success of every modern business. [1]. Anomaly detection is used outside of the medical sector to identify anomalous behaviour and discover irregularities in other domains, such as the detection of defects in safety-critical equipment and credit card fraud detection. Regardless, the technique of inconsistency area could give a high trickery rate and need expansive direction sets to get trustworthy execution results [2]. Data and correspondences innovation (ICT) frameworks, otherwise called Administrative Control and Information Obtaining (SCADA), are predictable with each other in spite of a high weakness to digital breaks. [3]. Due to the fact that a denial-of-service (DoS) attack inhibits communication through the categorization channels that have been adequately planned, this is the most secure solution currently known [4].

Learning a DoS attack allows one to easily demonstrate its features. [5].Muggers with different ways of thinking are often constrained by their energy, which means they may have to alter their assault strategy [6].

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

MOTIVATION AND PROBLEM DEFINITION

Due to its widespread popularity, the Internet is often the target of malicious cyberattacks. Cybersecurity in IDS is difficult since more and more people rely on web-based services. Because cybercriminals have easy access to data, we require data processing based on machine learning to combat cyber security threats. Intrusion detection analysis was developed to address weaknesses in conventional methods of Internet protection. Intrusion detection methods often have three major drawbacks: long detection times, poor accuracy, and inadequate adaptability The huge size and lopsided nature of the dataset represents a test for any AI based interruption location framework, prompting slanted discoveries and over-fitting. Consequently, appropriate feature learning and algorithms are required for accurate intruder entry diagnosis.

PROPOSED METHODOLOGY

We present an approach that uses a modified Deep Neural Network (MDNN) [8] and its associated parameter initialization and feature selection using adaptive Jaya optimisation (AJO) [9]. To better understand the diversity of cyber threats, an MDNN classifier is introduced. A Gravity Search Algorithm/Gray Wolf Optimisation (GSGW) hybrid is used to update the weight values in order to lessen the classification error. The primary objective is to combine the exploratory power of GSA with the exploitation potential of Grey wolf. The experimental results show that the hybrid algorithm can quickly converge to global optimums while also having a strong capacity to avoid local minima.

3.1Flowchart of the proposed System

Adaptive Jaya optimisation is used to select features from the NSL dataset in the proposed system. To distinguish penetration, the GSGW is used to figure the wellness esteem, which is then taken care of into the Changed profound brain organization.

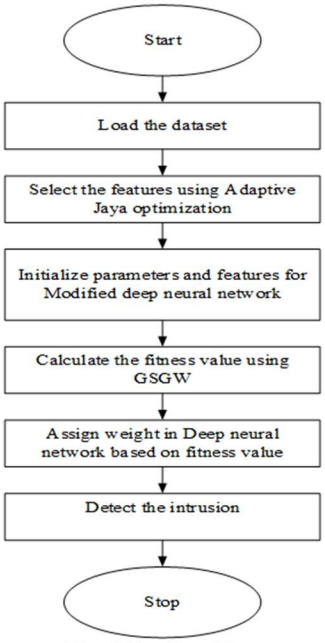


Figure1: Flow Chart of System

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

The NSL-KDD dataset is used in the suggested system. Fig.1 depicts the suggested system's flowchart. Right away, the information is stacked, and afterward the best elements are browsed the information utilizing the Versatile Jaya advancement technique. We feed the features to the Modified deep neural network in order to train it. Input, Stowed away, and Result are a couple of the layers that make up a profound brain organization. An information layer, four secret layers, and a result layer make up a changed profound brain organization. The result works on as the quantity of secret layers develops. The wellness esteem registered for each layer of the refreshed profound brain network is utilized to decide the weight esteem apportioned to that layer. The updated profound brain network utilizes the half and half Gravity search Calculation with Grey wolf optimisation (GSGW) to handle input values for each of the four secret layers, which brings about better results. The recommended approach further develops execution in identification rate while creating less misleading problems.

3.2 How the Grey Wolf Optimisation (GSGW) version of the Gravity Search Algorithm works on the MDDN

3.2.1 MDDN, or a modified deep neural network:

Even though a neural network only has one hidden layer, networks with many hidden layers, like those used in machine learning, are typically referred to as "deep learning."

For each weighted value in each layer, a hybrid gravity search algorithm (GSGW) and grey wolf optimisation (GWO) is used to determine the best-fitting value. Through Jaya improvement, the best highlights from the NSL-KDD dataset are chosen and utilized as info.

In the adjusted profound brain organization, let M location the amount of secret layers. In this manner, layer m fills in as the result endlessly layer 1 fills in as the information layer. Secret layers 2 and M-1 in the center are displayed in paint. Duplicating the worth by the heap (for this situation, W1, W2,..., Wm) yields the worth of every hub. Utilizing exploitation (GSGW), the redesigned deep neural network updates the load. The qualities at every hub are demonstrated by the documentation Ci,j. Since the system is rehashed for each layer, the qualities not entirely set in stone. The burden of each layer will be greater than zero. The network's complete interconnectedness is depicted in Figure 2.

$$\theta = \sum_{i=0}^{k} W_i X_i = W^T X$$

Each neuron in the hidden layer has its value determined and displayed as $Y_{i,} e^{\theta_k(i)}$

The upgraded profound brain network has four secret layers, as displayed in figure2. The performance benefits from having more hidden layers. For the aforementioned computation, we multiplied the GSGW-determined fitness value of 0.35 by a weight in the range [0, 1].

To mimic the human brain's pattern recognition abilities, neural networks are developed. Neural networks use machine learning to analyse data in the same way that human brains do. There are

no forms of communication that it cannot decipher. The neural network aids in data classification and clustering.

3.2.2 Grey-wolf optimisation added to a Gravity-based hybrid search method

A way to deal with molecule blend in light of gravity and mass is the gravitational search algorithm (GSA) [7]. This methodology relies upon Newton's law of development, which portrays the connection among power and speed. Objects in the vicinity are detected, and those with more mass and hence greater gravitational pull attract one another. If you want the greatest possible result, go with the heavier thing, and if you want the worst possible result, go with the lighter one. This algorithm is utilised as a detective in the proposed system to track down the trespasser. It gives the search orientation of the invader by describing the neighbouring system.

It is possible to write the formula as

$$F = k\frac{p1p2}{u^2}$$

Constant of Gravity = k

P1 -> Initial Mass

P2 = Secondary Object's Mass

U = Inter-Object Distance

The gravitational constant can be expressed with the help of this formula.

$$K(t)=K_0 e^{-\propto t/T}$$

At the outset, we set the values of K_0 and $\propto$.

The GSA algorithm picks agents at random according to factors like the mass and location of the items that make up the solution. In this case, we performed many iterations, with each one modifying the relative positions of the objects in terms of their speed, fitness, and acceleration.

The ith agent position in a system with M agents is defined as

$$Z_i = (z_i^1 .... z_i^h ..... z_i^m) \qquad for \quad i = 1,2,3 .... M$$

z_i^h demonstrates the h-th area of the specialist, ithagent, in the m-th layered space of pursuit.

Encourage applies equivalent power on the two masses I and j out of nowhere.

$$F_{ij}^h = k(t)\frac{p_{ai}(t)\times p_{sj}(t)}{d_{ij}+\varepsilon}(z_j^h(t)-z_i^h(t))$$

$k(t)$ ->Constant of gravity

$p_{ai}(t)$ -> Agent i's gravitational mass

$p_{sj}(t)$ -> Agent j's gravitational mass

ε -> stands for a very low constant

The separation of points i and j in Euclidean space looks like

$$d_{ij}(t) = \left|z_i(t).z_j(t)\right|$$

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

We can write the all out force identical on mass in the component at time t as a shorthand notation.

$$F_i^h(t) = \sum_{j \in kbest, j \neq i}^{M} random_j F_{ij}^h(t)$$

kbest is the requesting of the top k specialists regarding wellness, where is a genuine number in the reach [0,1].

The h-element's i-mass acceleration at time t is denoted as

$$a_i^h = \frac{F_i^h(t)}{p_{ii}(t)}$$

Where the mass of the $p_{ii}(t)$ of ith agent's inertia

A random number is multiplied with the object's current velocity and acceleration to get its new velocity. The formula for doing so is shown below.

$$q_i^d(t+1) = random_i q_i^d(t) + a_i^h(\mathrm{t})$$

$$z_i^d(t+1) = z_i^d(t) + q_i^d(t+1)$$

is a random number between zero and one

The populace is kept up-to-date through

$$p_{ai} = p_{sj} = p_{ii} = p_i \qquad i = 1,2,...M$$

$$p_i(t) = \frac{fitest_i(t) - worst(t)}{best(t) - worst(t)}$$

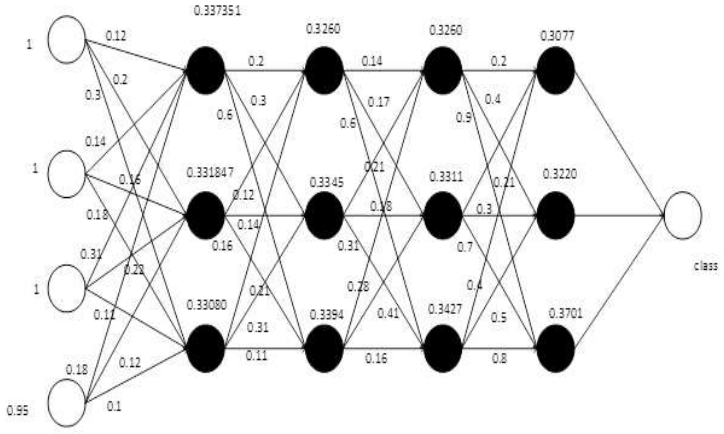


Figure2: Classifier based on an Adapted Deep Neural Network

The better profound brain organization's assault recipe is alluded to as

$$H = f(G_1^1 Z_1 \mid G_1^2 Z_2 \mid G_1^3 Z_3 \mid .....G_1^m Z_m)$$

$$H = f(\sum\nolimits_j G_i^j Z_j)$$

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

The quantity of neurons (addressed by Z) in the organization represents the heap (represented by G) on the connection between layers.

On all of the hidden layers of the updated deep neural network, the softmax function is utilized. Using the formula, we can determine the values.

$$P(y = j \mid \theta^i) = \frac{e^{\theta(i)}}{\sum_{j=0}^{k} e^{\theta_k(i)}}$$

Where

$$\theta = W_0 X_0 + W_1 X_1 + \ldots\ldots + W_k X_k$$

The most ideal incentive for Specialist I at Time t is meant by the image.

$$P_i(t) = \frac{p_i(t)}{\sum_{j=1}^{m} p_j(t)}$$

Use this formula to get the worst and best possible values:

$$best(t) = \min_{j \in (1 \ldots m)} fitest_j(t)$$

$$worst(t) = \max_{j \in (1 \ldots m)} fitest_j(t)$$

The method combines the particles based on the object's mass. The suggested technique use this algorithm to determine the object's heading, and then uses the grey wolf optimisation to continuously refine the location of that heading.Using the feature values from the NSL- KDD dataset, a fitness value is determined.

3.2.3 Grey wolf performance enhancement

The grey wolf algorithm represents group life and the leadership qualities of wolves. As a group, it sets out to hunt. The alpha wolf is the pack's leader, and the other wolves must obey his every order. The "beta" wolf, a subordinate member of the pack, aids the alpha wolf in making decisions. Alpha is the highest ranking wolf in the pack, while omega is the lowest. Delta represents a middle tier that falls between omega and alpha and is subservient to beta. The algorithm suggests a leader to go out and find the prey. When the alpha makes a hunting signal, the pack immediately begins searching for food. The subordinates follow the instructions to hide the game. At first, the wolf would surround its victim in order to establish a good attacking position. Next, the wolf's position is updated based on the current location of the prey.

There are several stages to the grey wolf algorithm [10].

Sa, b, Z, f, and itmax are search agents; initialise them together with the design variable size Sb.

$$\vec{Z} = 2\vec{b}.r_1 - \vec{b}$$

$$\vec{f} = 2.r_2$$

The value of b was halved between iterations.

• We can see the wolves as

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

$$\text{Wolves}=\begin{bmatrix} S_1^1 & S_2^1 & S_3^1 & \ldots & .. & .. & .. & S_{sb-1}^1 & S_{sb}^1 \\ S_1^2 & S_2^2 & S_3^2 & .. & .. & .. & .. & S_{sb-1}^2 & S_{sb}^2 \\ . & \ldots & .. & .. & \ldots & \ldots & \ldots & \ldots & \ldots . \\ . & \ldots . & \ldots . & \ldots . & \ldots & \ldots . & \ldots . & \ldots . & \ldots . \\ S_1^{sa} & S_1^{sa} & S_1^{sa} & \ldots & .. & \ldots & \ldots & S_{sb-1}^{sa} & S_{sb}^{sa} \end{bmatrix}$$

Where Sij is the starting point for the i-th wolf pack.

• The healthiness score is determined by

$$\vec{h} = \left| \vec{f} . \vec{S}_p(t) - \vec{S}(t) \right|$$

$$\vec{S}(t+1) = \vec{S}_p(t) - \vec{Z} . \vec{h}$$

- The finest hunting values must be determined.

$$\vec{h}_\alpha = \left| \vec{f}_1 . \vec{S}_\alpha - \vec{S} \right|$$

$$\vec{h}_\beta = \left| \vec{f}_2 . \vec{S}_\beta - \vec{S} \right|$$

$$\vec{h}_\delta = \left| \vec{f}_3 . \vec{S}_\delta - \vec{S} \right|$$

$$\vec{S}_1 = \vec{S}_\alpha - \vec{Z}_1(\vec{h}_\alpha)$$

$$\vec{S}_2 = \vec{S}_\beta - \vec{Z}_2(\vec{h}_\beta)$$

$$\vec{S}_3 = \vec{S}_\delta - \vec{Z}_3(\vec{h}_\delta)$$

It is possible to determine the wolf's current position using

$$\vec{S}(t+1) = F \frac{\vec{S}_1 + \vec{S}_2 + \vec{S}_3}{3}$$

Combining the gravity search method's F value with the grey wolf algorithm improves performance. Until the condition is met, the fitness value is recalculated, and the positions are updated accordingly.

3.2.3.1 The GSGW Algorithm Calculation:

Fitness

[38978.26003331 73779.0372579 78484.95302316 838326.5630996 24337.66872029 147618.91102804 23099.83020553 48373.99988401 13028.99315072 127280.69518529 87722.61209052 28510.70901802 39233.56175001 29292.9189462 357570.22205822 111550.93472763 19303.52557341]

Worst: 838326.5630995962

Best: 13028.9931507225

First: 0.9685576841281687

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

0.0673258627956637 seconds

Eps =2.220446049250313e-16

A Random Number Generator Gave Me = 171.74815363608246

To calculate the distance, we use the formula: 1.

Dij= 37.62388831350286 *21.496048611951167 = 808.7649321576789

IV.The recommended strategy utilizes the versatile jaya advancement procedure to choose the best highlights from the NSL-KDD dataset. The principal estimations are according to the accompanying: administration, Src and DST bytes, hot, num_root, protocol_type, num_file_creations, count, banner, srv count, num_compromised, dst have count, dst have srv count, rerror rate, term, dst have srv count, signed in The best characteristics that were chosen to identify various cyber security attacks are fed to the redesigned neural network.

RESULTS AND DISCUSSIONS:

We advise using AJOMDNN-GSGW because it yields superior DR, low FAR, and good accuracy.

Table 2: Attacks using feature selection and those that don't

The improved deep neural network's top features, as chosen by Adaptive Jaya optimisation, are listed below. The qualities in the NSL-KDD dataset are recorded by field number in the table.

class	1) By AJOMDNN-GSGW without FS						2) By AJOMDNN-GSGW with FS					
	Predicted attack						Predicted attack					
	R2L	Probe	Normal	U2R	DoS	DR	R2L	Probe	Normal	U2R	DoS	DR
R2L	2732	8	4	7	3	98.55	2743	4	4	2	1	99.52
Probe	0	0	1	199	2	98.68	0	0	1	201	0	99.38
Normal	22	13	14	18	7389	99.74	5	4	4	6	7437	99.87
U2R	6	2400	6	5	4	83.26	2	2407	5	4	3	91.78
DoS	12	11	9663	10	14	99.68	6	7	9684	6	7	99.85

The intruder will do a scan of the system as a probe to learn more about it.

Denial of service (DoS): The attack uses up system resources, rendering the workstation unusable to the user.

U2R, or user-to-root: The hacker successfully gained root access and then attempted to exploit the system's elevated privileges.

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

Distant to end-user (R2L): The intruders transmit packets via the network in an attempt to reach the remote and exploit the system.The trespasser is not registered on the local network.

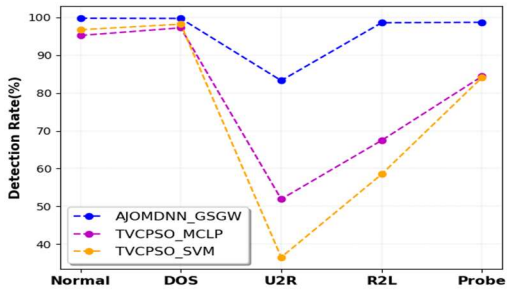


Figure 3: Dynamic Range without Feature Selection

Table 1

Our proposed system's top feature selections from the NSL-KDD dataset are shown in Table1.

Basic features	{1,2,3,4,5,6}
Content features	{10,12,13,16,17}
Features of Time based	{23,25,28}
Features of Host based	{32,33,36}

Location rate appraisal without highlight determination is displayed in Fig 3.The suggested approach is called AJOMDNN_GSGW. When compared to traditional approaches, it demonstrates an improved detection rate of 95.98%. The detection rates without feature selection for the various assaults discussed here (Normal, DOS, U2R, R2L, Probe) were 99.74, 99.68, 83.26, 98.55, and 98.68.

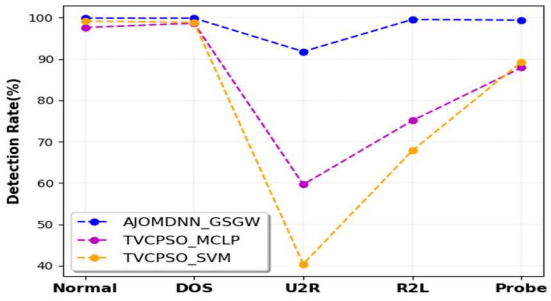


Figure 4: Feature selection for DR

In Fig., the discovery rate following element choice is assessed and shown. 4. Features are picked using AJO on the NSL-KDD dataset. Overall, it outperforms previous approaches by a margin of 98.07 percent in terms of detection. The discovery rates accomplished were 99.87 percent for Ordinary assaults, 99.85 percent for DOS assaults, 91.78 percent for U2R assaults, 99.52 percent for R2L assaults, and 99.38 percent for Test assaults.

When the two graphs depicting the different attacks are compared, the one depicting the attacks using feature selection demonstrates a higher detection rate. Existing TVCPSO methods, like TVCPSO-MCLP and TVCPSO-SVM, are stood out from the proposed method for managing highlight its benefits [1].

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

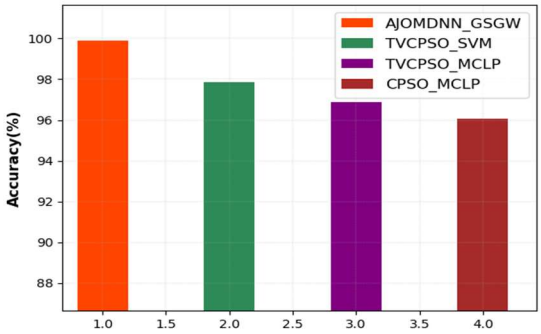


Figure 5: Exactness independent of feature selection

The accuracy assessment performance of our suggested system is shown in Fig 5. The accuracy is uncovered separated from highlight determination. AJOMDNN_GSGW has a 99.71 percent higher precision rate than the past techniques TVCPSO-MCLP, TVCPSO-SVM, and CPSO-MCLP.

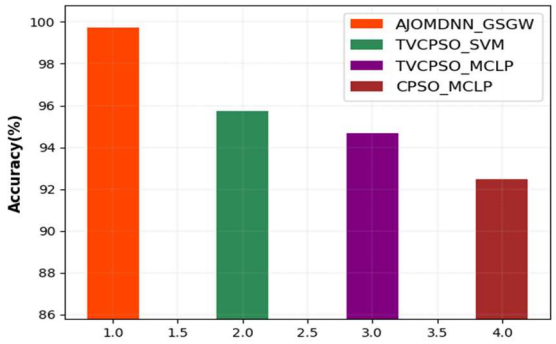
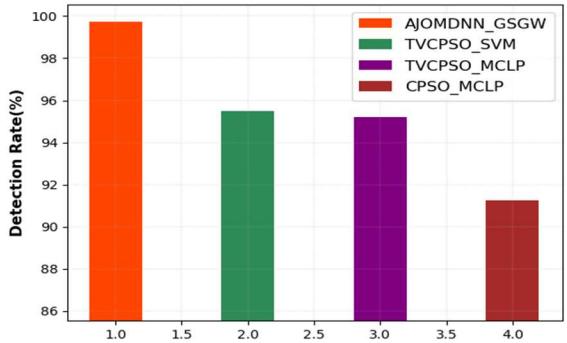


Figure 6: Selected features are accurate.

The accuracy assessment performance of our suggested system is shown in Fig 6. It demonstrates how well feature selection may work. AJOMDNN_GSGW has a higher precision level of 99.87 when contrasted with TVCPSO-MCLP, TVCPSO-SVM, and CPSO-MCLP, which were the past strategies. Features are picked using AJO on the NSL-KDD dataset. The diagram that is shown is more precise with include choice than it is without it. Existing methods like TVCPSO-MCLP (Time changing tumult atom swarm improvement various models straight programming), TVCPSO-SVM, and CPSO-MCLP(chaos particle swarm smoothing out) are stood out from the proposed system. The recommended strategy is the versatile Jaya advancement changed profound brain organization - gravity search dim wolf calculation (AJOMDNN-GSGW).



Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

Figure 7: Dynamic Range without Feature Selection

In Fig., the location pace of our recommended framework without highlight choice is assessed. 7.With a detection rate of 95.98%, AJOMDNN_GSGW outperforms its predecessors, TVCPSO-MCLP, TVCPSO-SVM, and CPSO-MCLP, which achieve rates of 94.69, 95.75, and 92.47 percent, respectively.

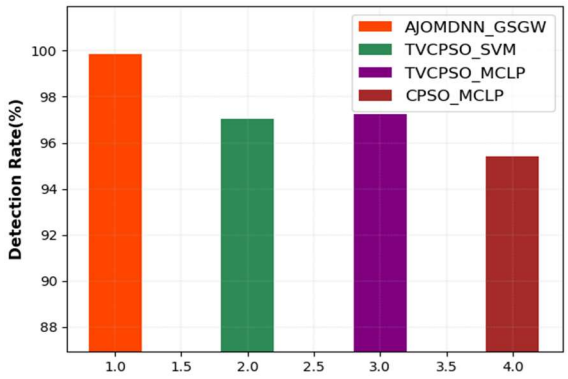


Figure 8: Feature-less Feature-Based DR

The discovery rate assessment for our proposed framework with highlight determination is displayed in Fig 8. When compared to the detection rates of the older techniques TVCPSO-MCLP (representing 94.69), TVCPSO-SVM (representing 95.75), and CPSO-MCLP (representing 92.47), With a higher detection rate of 98.07%, AJOMDNN_GSGW stands out.

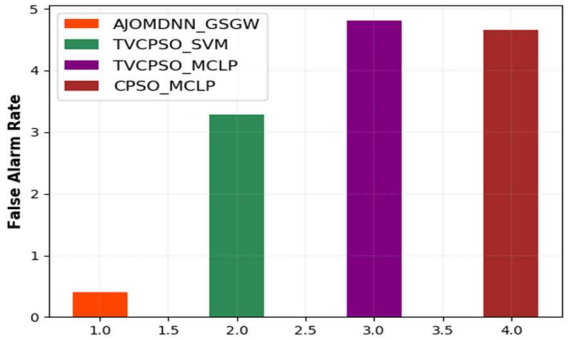
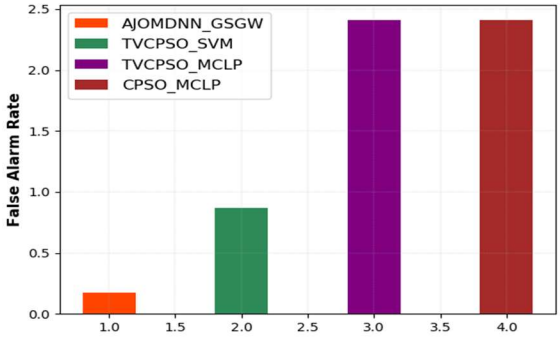


Figure 9: Without selecting features, FAR

The FAR performance assessment of our suggested system without FS(FeatureSelection) is shown in Fig. 9. When compared to the TVCPSO-MCLP technique (4.81), the TVCPSO-SVM method (3.29), and the CPSO-MCLP method (4.66), AJOMDNN_GSGW shows a low FAR of 0.0028%.



Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1213-1225

Figure 10: Feature selection in FAR

The FAR performance assessment of our suggested system using FS is shown in Fig 10.When compared to the prior approaches With a FAR as low as 0.0012% in TVCPSO-MCLP, TVCPSO-SVM, and CPSO-MCLP, AJOMDNN_GSGW stands out.

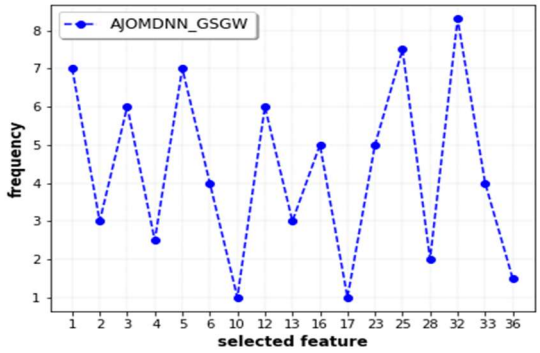


Figure 11: AJO-based Feature Selection

Table7 illustrates the frequency with which certain attributes are employed in the proposed system, and Fig.11 depicts this data. Feature selections made using AJO on the NSL- KDD dataset are shown along the x-axis.

Table 3: Proposed Method Parameters

Variables	Values for AJOMDNN-GSGW
Maximum iteration	400
Particles used	17
Range values of F	[0,1]

We utilised the aforementioned values in the recommended approach throughout our implementation of this research. The differences and similarities between the suggested approach (AJOMDNN-GSGW) and the currently used methods are laid forth in Table 4.

Table 4: Examining the Proposed Method Against the Current [1]

Metrics	TVCP-MCLP	TVCP-SVM	CPSO- MCLP	AJOMDNN-GSGW
Parameter without selected feature				
Accuracy	94.69	95.75	92.47	**99.71**
Detection rate (DR)	95.19	95.49	91.26	**95.98**
False alarm rate (FAR)	4.81	3.29	4.66	**0.0028**
Parameter with selected feature				
Accuracy	96.88	97.84	96.06	**99.87**
Detection rate (DR)	97.23	97.03	95.42	**98.07**
False alarm rate (FAR)	2.41	0.87	2.41	**0.0012**

CONCLUSION & FUTURE WORKS:

In this research, we provide a method that can init parameters and FS for an MDNN all at once using a clever intrusion detection setup and Adaptive Jaya Optimisation (AJO). We provide a

multi-layer neural network (MDNN) classifier for categorizing potential threats to network security. To reduce classification errors, weight value updates are calculated using a Gravity Search Algorithm and Gray Wolf Optimisation (GSGW) combination. To do this, we used the KDD cup enlightening file's best 17 components for high DR and low FAR. Picking another arrangement of qualities utilizing an alternate strategy may be useful for future work.

REFERENCES

[1] Bamakan, SeyedMojtaba Hosseini, Huadong Wang, Tian Yingjie, and Yong Shi. "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization." Neurocomputing 199 (2016): 90-102.

[2] Ji, S.Y., Jeong, B.K., Choi, S. and Jeong, D.H., 2016. A multi-level intrusion detection method for abnormal network behaviors. Journal of Network and Computer Applications, 62, pp.9-17.

[3] Hong, J. and Liu, C.C., 2019. Intelligent electronic devices with collaborative intrusion detection systems. IEEE Transactions on Smart Grid, 10(1), pp.271-281.

[4] Amin, S., Cárdenas, A.A. and Sastry, S.S., 2009, April. Safe and secure networked control systems under denial-of-service attacks. In International Workshop on Hybrid Systems: Computation and Control (pp. 31-45). Springer, Berlin, Heidelberg.

[5] Zuba, M., Shi, Z., Peng, Z. and Cui, J.H., 2011, December. Launching denial-of-service jamming attacks in underwater sensor networks. In Proceedings of the Sixth ACM International Workshop on Underwater Networks (p. 12). ACM.

[6] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, “Cyber security of water scada systems-part i: Analysis and experimentation of stealthy deception attacks,” IEEE Transactions on Control Systems Technology, vol. 21, no. 5, pp. 1963–1970, 2013.

[7] Rashedi E, Nezamabadi-pour H and Saryazdi S (2009) GSA: a gravitational search algorithm. Inform. Sciences. 179(13), 2232-2248.

[8] Thupakula Bhaskar, Tryambak Hiwarkar, K. Ramanjaneyulu. A Modified Deep Neural Network Based Hybrid Intrusion Detection System in Cyber Security, IJITEE, ISSN: 2278-3075, Volume-8 Issue-8, June 2019.

[9] Thupakula Bhaskar, Tryambak Hiwarkar, K. Ramanjaneyulu.A novel approach for feature selection technique in NSL-KDD data set of cyber security, IJAAI,Volume 6, Issue 6, June 2019.

[10] E. Emary, Hossam M. Zawbaa, and CrinaGrosan Experienced Gray Wolf Optimization through Reinforcement Learning and Neural Networks. IEEE transactions on neural networks and learning systems, vol. 29, no. 3, march 2018.