Received: July 15, 2023. Revised: August 14, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Enhanced PSO Algorithm for Detecting DRDoS Attacks on LDAP Servers

Riyadh Rahef Nuiaa[1]* Saif Ali Abd Alradha Alsaidi[1] Bahaa Kareem Mohammed[2]
Ali Hakem Alsaeedi[3] Zaid Abdi Alkareem Alyasseri[4,5] Selvakumar Manickam[6]
Mohammed Abdulridha Hussain[7]

[1]Department of Computer/college of education for pure sciences / Wasit University, Wasit, Iraq
[2]Department of Electrical Techniques, Technical Institute Kut Middle Technical University Baghdad, Iraq
[3]College of Computer Science and Information Technology, Universitas of Al-Qadisiyah, Al-Qadisiyah, Iraq
[4]Information Technology Research and Development Center (ITRDC), University of Kufa, Najaf, Iraq
[5]College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq
[6]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
[7]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
* Corresponding author's Email: riyadh@uowasit.edu.iq

Abstract: In recent years, there has been an increase in distributed reflective denial of service (DRDoS) attacks, particularly those that target open lightweight directory access protocol (LDAP) servers. These attacks involve transmitting a small request to a large number of available LDAP servers, seeking information from all users. Consequently, the servers respond with significantly more data than the original request, amplifying the traffic and overwhelming the target with massive amounts of data. Therefore, this paper proposes a novel model for detecting LDAP-based DRDoS attacks by utilizing an enhanced particle swarm optimization (PSO) algorithm based on an adaptive weighted threshold (AWTPSO) model. The proposed AWTPSO model incorporates network traffic features and LDAP protocol characteristics to identify attack patterns. It further employs an adaptive weighted threshold model to dynamically adjust the threshold value for each feature. The enhanced PSO algorithm optimizes the threshold values, thereby improving the detection accuracy of the proposed model. The proposed AWTPSO detection model has been validated using the recent CICDDoS2019 dataset (LDAP sub-dataset). The experimental results demonstrate that the AWTPSO model effectively detects LDAP-based DRDoS attacks with exceptional accuracy of 99.99% and minimal false positives of 0.01%, surpassing other state-of-the-art techniques. Consequently, the proposed model presents a highly promising and robust solution for detecting the threat of LDAP-based DRDoS attacks on enterprise networks.

Keywords: LDAP DDoS attacks, Adaptive weight threshold, Feature selection, Cybersecurity attacks, Enhancing PSO, AWTPSO.

1. Introduction

Over the past decade and in the current computing era, users have increasingly used mobile and handheld devices [1]. To access financial services, network resources, online shopping platforms, retail outlets, games, and media content, you can utilize the internet. Companies have made their services accessible to users from any location to increase their revenue through web applications. In addition, there has been a significant increase in internet subscribers and connected devices in recent years, and the number of users utilizing web applications to access services and perform specific tasks has witnessed a notable increase. However, this rapid expansion has created insecure network routes and non-secure connected devices [2, 3]. Businesses and funds are lost. In the financial and retail sectors, the availability and quality of service for legitimate users are of utmost importance. These services can be disrupted or interrupted by a massive influx of malicious traffic aimed at web applications. Therefore, hackers employ several tools or programs to generate a flood of malicious traffic and launch attacks against the

victim system [4]. Hackers primarily employ denial of service (DoS) and distributed DoS attacks to disable or degrade the performance of services.

Attackers always exploit vulnerabilities in security systems, network protocols, or cybersecurity workers' lack of security awareness. Over the years, several LDAP vulnerabilities have been reported, various security vulnerabilities have been identified in different independent LDAP implementations, encompassing Denial of Service attacks, remote code execution, and privilege escalation. Furthermore, LDAP has more recently been exploited in volumetric attacks, specifically distributed reflective denial of service (DRDoS) attacks, with a focus on utilizing the lightweight directory access protocol (LDAP). In these attacks, the assailant sends many LDAP queries to susceptible LDAP servers while masquerading as normal LDAP clients with fake IP addresses. As a result, the LDAP server becomes too busy to generate replies for the attacker and cannot reply to legitimate LDAP clients [5].

Multiple vulnerabilities exist in the implementation of the lightweight directory access protocol (LDAP) protocol, which can potentially enable an unauthenticated remote attacker to induce a device reload, leading to a distributed reflective denial of service (DRDoS) condition [6]. These vulnerabilities stem from the incorrect handling of LDAP messages by affected devices. Exploitation of these weaknesses involves sending an LDAP packet to a vulnerable device, with the LDAP message containing the source IP address of an LDAP server configured on the targeted device. In the event of a successful exploit, the compromised device will undergo a reload, resulting in a DRDoS state [7, 8].

To launch volumetric LDAP-based DRDoS attacks, attackers utilize LDAP servers that provide UDP (user datagram protocol) services. By leveraging LDAP queries via UDP, the amplified reflection-based LDAP attack creates massive amounts of traffic. The attacker initiates the attack by sending an LDAP request to an LDAP server, in which the sender IP address is spoofed to resemble the target's IP address. The server answers the victim's IP with a bulked-up response, resulting in the reflection attack [9]. The victim's computer cannot handle enormous amounts of LDAP data simultaneously [10].

The main contributions of the proposed model are as follows:

- Named AWTPSO, the model is specifically designed to detect LDAP-based DRDoS cyberattacks targeted at the active directory.
- By integrating adaptive threshold and optimization algorithms based on machine learning, the AWTPSO model offers comprehensive protection against DRDoS cybersecurity attacks directed at the LDAP directory service.
- Leveraging particle swarm optimization (PSO) in conjunction with adaptive thresholding, the AWTPSO model effectively selects salient features surpassing the threshold, thereby enabling the detection of DRDoS cybersecurity attacks directed at LDAP packets while ensuring the continuity of active directory functions during an attack.
- The detection model is implemented using the decision tree algorithm to assess and classify network traffic into normal or abnormal categories.
- The proposed AWTPSO detection model is meticulously designed and rigorously validated using the CICDDoS2019 dataset.
- Comparative analysis showcases the remarkable performance of the proposed AWTPSO model, achieving exceptional detection accuracy along with an impressively low false positive rate.
- Additionally, the proposed AWTPSO model boasts a highly scalable and loosely-coupled architecture, further augmenting its applicability and efficiency in cybersecurity settings.

The remaining sections of this study are structured as follows: Section 2 reviews the related works. Section 3 provides the preliminaries. Section 4 outlines the methodology of the proposed model and presents the results and discussion. The conclusion of the work is presented in section 5.

2. Related works

In today's interconnected world, researchers consider detecting and mitigating cyber threats, including DDoS attacks, an important area of research. Organizations that use LDAP for identity and access management are at significant risk due to the increasing prevalence of DDoS attacks against the LDAP directory service. Researchers have proposed various approaches to detect and protect against such attacks, ranging from rule-based systems to machine learning algorithms. This section reviews relevant studies, highlighting their strengths and limitations.

According to [4], the experiment employs the Spark methodology on cluster nodes for the purpose of feature selection and classification of DDoS attacks. The proposed approach is specifically designed to classify diverse types of DDoS attacks by utilizing feature selection techniques. Notably, this approach successfully classifies the LDAP DDoS attack as one of the identified attack types.

As indicated by [11], the proposed N-tier machine learning-based architecture for identifying DDoS attacks is an innovative framework that leverages classifiers as the primary machine learning techniques to construct training data. This framework is divided into two distinct phases: preprocessing and feature selection, which are succeeded by feeding the processed data into the second phase to generate an attack model utilizing machine learning techniques. In order to compute the significance of each feature within the dataset, consisting of 88 features, the Random Forest Regressor is employed. From the initial CICDDoS2019 dataset, a subset of 24 features is carefully selected to train the model.

According to [12], DIDDOS is a DDoS detection framework that combines deep learning (DL) and machine learning (ML) techniques. The framework utilizes a gated recurrent unit (GRU), which is a type of recurrent neural network (RNN) in deep learning, along with machine learning algorithms such as sequential minimal optimization (SMO) and Naive Bayes (NB). The research study was conducted on the CICDDoS2019 LDAP dataset, which is a subset of the CICDDoS2019 dataset. Among the models used, the SMO model achieves the highest accuracy of 99.96%, followed by the GRU, RNN, and NB models with accuracies of 99.95%, 99.94%, and 99.82%, respectively.

According to [13], a DDoS defense strategy for software-defined networking (SDN) is proposed, incorporating bandwidth control mechanisms and the XGBoost algorithm. This solution utilizes an adaptive threshold methodology and a bandwidth control algorithm to regulate network traffic. By employing multiple bandwidth profiles, the adaptive threshold value becomes more adaptable and precise in accounting for network traffic variations, thereby reducing the packet failure ratio. The experiment conducted in this paper demonstrates that the utilization of multiple bandwidth profiles significantly reduces the packet loss ratio from 23.85% to 2.16%, as compared to a single profile-based threshold. Among all the evaluated algorithms using the CICDDoS2019 (LDAP) dataset, the XGBoost model achieves the highest precision, recall, and F1-measure.

This study [14] aims to prevent DDoS attacks on transport data by using smart contracts to record local transport system events on the blockchain. The model uses an autoencoder and a multi-layer perceptron to detect DDoS attacks using deep learning techniques. The multi-layer perceptron utilizes the softmax function in the final layer as an activation function to classify DDoS attacks, while the learned autoencoder extracts features. Unsupervised learning helps the autoencoder recognize data representations. Data flows from the input to the output layers in the multilayer perceptron, which is a feed-forward network. In contrast to the autoencoder, the multi-layer perceptron consists of one input layer, one output layer, and one or more hidden layers. Multilayer perceptrons use hidden layers to compute. However, the bottleneck layer reduces complexity by having fewer nodes. Hidden layers activate with RELU functions. Recursive feature reduction improved the model's efficiency.

3. Preliminaries

3.1 Feature selection

Feature selection is the most important and best strategy that exists to reduce data dimensions and has been used for numerous real-world problems. In the scenario of a dataset that may contain noisy, irrelevant, or redundant attributes [15, 16], it often slows down and even degrades the accuracy of a learning system [17]. A feature selection algorithm plays a crucial role in minimizing the number of attributes, reducing learning time, and improving the classification performance of algorithms by eliminating unnecessary and redundant features. Thus, feature selection becomes an essential process in identifying the most consistent, non-redundant, and relevant attributes for model creation [18]. With the increasing number and diversity of datasets, it becomes imperative to systematically reduce them. Therefore, feature selection aims to pick certain essential attributes from the initial feature set that will increase the effectiveness of a predictive model and lower the computational cost of modeling [19]–[21].

3.2 The particle swarm optimization (PSO)

Animal social behavior primarily influenced the basic ruling, such as fish schooling and bird flocking. The birds move from one location to another in search of food, and the birds can smell food wherever it is available. The bird knows its surroundings and uses them to locate and manage food resources[22].

Table 1. CICDDoS2019 (LDAP) dataset details

Dataset	Abnormal	Normal	Total
CICDDoS2019 (LDAP DDoS attack) train.	183489	200915	384404
CICDDoS2019 (LDAP DDoS attack) test	59714	68427	128141

The global optimization approaches are used to calculate the learning approach from the animal's behavior, where the swarm or crowd will be known as a particle [23, 24]. The PSO technique updates the Eq. (1) and determines each partner's position in the crowd for searching the space globally Eq. (2).

$$v_{id+1} = v_{id} + c_1 r_1 (p_{id} - x_{id}) + c_2 r_2 (g_{best} - x_{id}) \quad (1)$$

Where v_{id} is the velocity vector of particle, x_{id} is particle's vector position, P_{id} is personal best position of particle, g_{best} is the global best position of particle *t* is the time of initialization, *c1*and *c2* are positive acceleration constants, *r1* and *r2* are random numbers and can be computed by the equation:

The proposed equation below can use the adaptive threshold as a fitness function in PSO to improve the feature selection method:

$$V_{id}(t+1) = w * V_{id} + c1 * rand1() * (P_{best_{id}} - X_{id}) + c2 * rand2() * (g_{best} - X_{id}) \quad (2)$$

$$X_{id}(t+1) = X_{id} + V_{id} \quad (3)$$

In Eqs. (1, 2), X_{id} and V_{id} are new position and velocity for particle *i*, respectively. P_{best} is the best solution vector of particle *i* and the best solution of system is the g_{best} *rand1()* and *rand1()* are a random number between (0, 1). *cl*, *c2* are learning factors (usually *cl* = *c2* = 2). *w* is an inertia weight.

3.3 Dataset

The CICDDoS2019 dataset is currently the most popular and up-to-date dataset used for DRDoS attacks [25]. It includes both benign and advanced DRDoS attacks. The dataset includes the latest reflective DDoS attacks. It also has application-layer DDoS attacks that use TCP and UDP protocols based on reflection and exploitation. The CICDDoS2019 (LDAP DRDoS) dataset contains 88 network characteristics. Table 1 provides more details about the CICDDoS2019 (LDAP) dataset, including the training and test groups' size and normal and abnormal traffic.

4. Proposed LDAP DDoS detection model

The LDAP-based DRDoS attack is a type of distributed reflective denial of service (DRDoS) attack that targets open lightweight directory access protocol (LDAP) servers. In this attack, the attacker sends spoofed requests to open LDAP servers, asking for information on a particular user or object. The server then responds with a much larger amount of data than the original request, amplifying the traffic and flooding the target with a massive volume of data. This can cause the target's network to become overloaded and unavailable to legitimate users. The attack is effective because LDAP servers are often misconfigured and left open to the public, allowing attackers to easily exploit them. The LDAP-based DRDoS attack has been used by cybercriminals to launch large-scale attacks on businesses and organizations, causing significant damage to their reputation and operations. To detect this attack, it is important to secure LDAP servers and restrict access to them only to authorized users. As a result, we have proposed the LDAP DRDoS Detection model, illustrated in Fig. 1. This model comprises three stages: data preprocessing, feature selection, and classification and detection. The purpose of the proposed model is to identify LDAP DRDoS attacks that operate at the application level, employing TCP, UDP, or a combination of both. These attacks exhibit distinctive network traffic features that can be distinguished from normal or other DRDoS attack traffic.

4.1 Data preprocessing

The network traffic captured is raw data, which may contain missing, NaN, and infinite values. Feature selection techniques and machine learning classifiers cannot operate on such noisy datasets. Therefore, the raw data is first cleaned and preprocessed [26] to make it suitable for the operation of classifiers and feature selection techniques. Data preprocessing (data cleaning) is described by Algorithm 1, and this stage yields results in the elimination and reduction of noise in a dataset. First, duplicate instances in the dataset are removed. Then, missing and infinite values are replaced with the mean for those features. After the data cleaning process is complete, the data is rescaled within the range of 0 to 1 or -1 to 1 using data normalization [27]. The equation is as follows:

$$x_{\text{normalized}} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (4)$$

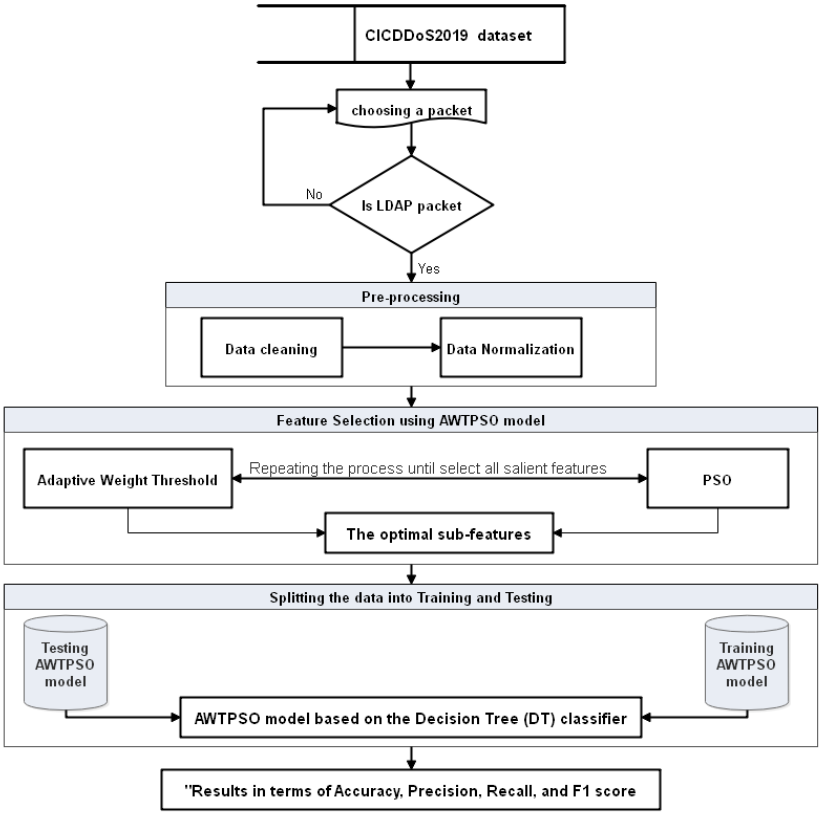

Figure. 1 The diagram for the proposed AWTPSO model

Algorithm 1: Data pre-processing (data cleaning)

$input: C\ ICDDoS2019(LDAP) dataset\ with\ feature\ subset$
$output: compact\ dataset$
$f(N) = n_1, n_2, n_3, n_4, \ldots, n_n$
$for\ n \leftarrow\ in\ CICDDOS2019(LDAP) dataset\ do:$
  $if\ n\ contains\ duplicate\ features\ then:$
    $removed$
  $elseif\ n\ contains$ infinite $values\ then:$
    $replace\ with\ mean\ for\ that\ feature$
  $elseif\ \ n\ contains$ missing $values$ " $blank\ cell$" $then:$
    $replace\ with\ mean\ for\ that\ feature$
$return\ f(M) =\ \ m_1, m_2, m_3, m_4, \ldots, m_m$." $feature\ after$ Pre-processing"

Therefore, the process of data preprocessing produces a dataset that has been cleaned and normalized, making it suitable for reducing features.

The feature selection stage is designed based on suggesting a new fitness function (adaptive weighted threshold) for the PSO algorithm. In the context of PSO, particles represent candidate solutions in the search space, and each particle maintains its personal best (P_{best}) and the global best (g_{best}) positions found by the entire swarm.

The adaptive threshold is calculated as a weighted combination of the statistical properties of the feature values (μ and α) and the difference between the personal best and global best positions of the particles, with the weight parameter w controlling the influence of the PSO optimization on the threshold.

The Eq. (5) allows the PSO algorithm to dynamically adjust the threshold during the feature selection process based on the convergence progress of the particles. A higher value of w will give more weight to the PSO optimization, potentially leading to a more aggressive threshold update, while a lower value of w will put more emphasis on the statistical properties of the feature values.

$$Th = (1 - w) * (\mu + k * \alpha) + w * (p_{best} - g_{best}) \quad (5)$$

Algorithm 2: An adaptive weighted threshold PSO(AWTPSO) feature selection model

```
input: load the dataset
output: optimal features
th ← 0.1// initially set the threshold (th = 0.1)
k ← 0 //is a user defined constant that determines the th sensitivity.
while itr_cunt ≤ itr_max do:
    for each feature (x) in dataset do:
        update the population according to the optimization method
        update the velocity using equation(1)
        update the position using equation (2)
        if p_best(th) < p_best then:
            p_best ← p_best(th)
            update the th based on equation (5,6)
            k ← 0
        elseif g_best(th) < g_best then:
            g_best ← g_best(th)
            update the th based on equation (5,6)
        else :
            k ← k + 1
    elseif k ≤ 2 * populationsize then :
            k ← 0
            th ← It is selected randomly by the user (algorithm 3)
Return optimal features
```

Table 2. The true and negative class predictions based on the AWTPSO model

Metrics	TP	FP	FN	TN
Samples number	64960	7	12	63162
Classification percentage	99.9815	0.0111	0.0185	99.9889

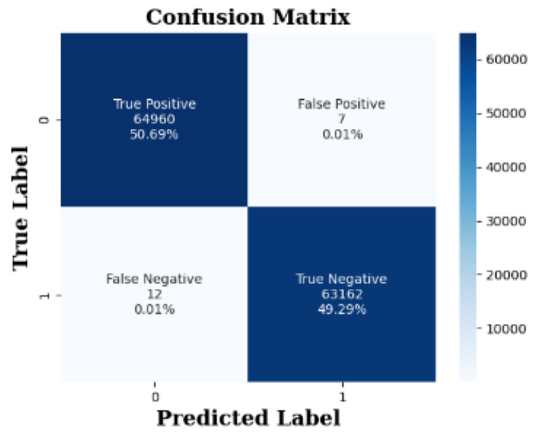

Figure. 2 Confusion matrix for the proposed model

Where: μ is the mean of the feature values in the dataset; α is the standard deviation of the feature values in the dataset; *k* is a user-defined constant that determines the threshold's sensitivity.

W is the weight parameter that determines the balance between the g_{best} and P_{best} of the particles in the PSO algorithm that can be calculated by the below equation:

$$w = w_{max} - ((w_{max-}w_{min}) * (\frac{itr_{cunt}}{itr_{max}})) \quad (6)$$

Where W_{max} is the initial value of the inertia weight at the beginning of the optimization process.

W_{min} is the final value of the inertia weight at the end of the optimization process. itr_{cunt} is the current iteration number of the PSO algorithm. itr_{max} is the total number of iterations or maximum number of generations set for the PSO algorithm.

This equation starts with a higher initial inertia weight value W_{max} and linearly decreases it to a lower value W_{min} as the algorithm progresses through iterations *itr* towards the maximum number of iterations itr_{max} This allows the particles to explore the search space more broadly at the beginning and converge towards the global best or personal best solutions at the end, striking a balance between exploration and exploitation in the optimization process. can adjust the values of W_{max} and W_{min} to control the balance between the global best and personal best influences on the particles' movement in the PSO algorithm, depending on your specific optimization problem and requirements.

Algorithm 3: Adaptive threshold (th)

```
select_x = []
for i in range (length (p)) do:
    if p[i] > th then:
        select_x.append(i)
fit = evaluate_fit(select_x) // Evaluate fitness using selected features
if fit > pre_fit then:   // update the threshold
    th = th_inc // increment threshold
else:
    th = th_dec // decrement threshold
Return fit
```

Table 3. the classification performance metrics of the proposed AWTPSO model based on the DT classifier.

Metrics	TP	FP	FN	TN
AWTPSO	0.9999	0.9999	0.9998	0.9999

Table 4. A Comparison of the proposed AWTPSO model with other LDAP-based DRDoS attack detection works

System	Accuracy	Precision	Recall	F1score
SSK-DDoS [4]	94.42	96.00	73.00	83.00
multi-tier [11]	Not mention	62.2	28.6	39.2
DIDDoS [12]	99.96	99.71	99.91	99.87
Bandwidth Control Mechanism [13]	Not mention	86.00	96.00	91.00
hybrid deep learning [14]	Not mention	91.00	99.00	95.00
AWTPSO (our model)	99.99	99.99	99.98	99.99

In this pseudocode (Algorithm 3), particle *P* is a binary array representing the selected features *select_x* in the current iteration of PSO. The threshold *th* starts at an initial value, and previous_fitness *pre_fit* is the fitness *fit* of the particle *P* in the previous iteration. Threshold_increm *th_inc* and threshold_decrement *th_dec* are hyperparameters that determine how much the threshold *th* should be adjusted based on the fitness *fit* improvement.

The adaptive threshold fitness function first selects the features whose values are above the threshold. Then, it evaluates the fitness of the particle using the selected features. If the fitness improves compared to the previous iteration, the threshold is increased, otherwise, it is decreased. This helps to adapt the threshold to the changing fitness landscape and potentially speeds up the convergence of PSO.

Table 2 presents the model's ability to correctly predict and wrongly predict when checking the LDAP packet.

Fig. 2 presents the confusion matrix result for the proposed (AWTPSO) model.

The model has correctly identified 64960 of the total 128141 samples as LDAP DDoS attack packets. It has also correctly identified 63162 samples as benign LDAP packets. But the model misidentified 7 benign LDAP packets as LDAP DDoS attack packets when it should have known better. On the other hand, the model got 12 samples of LDAP DDoS attack packets wrong, and they were wrongly labeled as benign LDAP packets.

The proposed model has been evaluated based on several accuracy metrics such as Accuracy, Precision, Recall, and F1score, and the results in the below table indicate that the AWTPSO model proposed achieved higher accuracy metrics than models that exist in the literature. Table 3 presents the results obtained from training the AWTPSO model proposed with the DT classifier based on classification performance metrics.

We are comparing the AWTPSO model proposed with other state-of-the-art approaches in Table 4 based on their classification performance metrics.

In our proposed AWTPSO model, we used popular and famous metrics to evaluate it, and those classification performance metrics. Therefore, our AWTPSO model proposed will be compared with related works that exist in the literature based on the metrics mentioned above.The first metric is accuracy; among all the related works that exist in the literature review and that used the same dataset, there are only two that mention accuracy in their works. According to [4], they suggest an SSK-DDoS system, and the highest accuracy obtained is 94.42%, as well as,

according to [12], the proposed DIDDOS approach, and the highest accuracy obtained is 99.96% for the LDAP attacks. Meanwhile, our proposed AWTPSO model obtains higher accuracy than both previous models, which is 99.99% using the same conditions. Therefore, the proposed AWTPSO model is the best in terms of accuracy.

The second metric is precision. According to [4], they suggest an SSK-DDoS system, and the highest precision obtained from their system is 96.00%, while the multi-tier model suggested by [11] has obtained the highest precision at 62.2%, whereas the DIDDOS approach suggested by [12] has obtained the highest precision at 99.71%. In the same manner, the bandwidth control mechanism proposed by [13] has obtained the highest precision of 86.00%, while the hybrid deep learning approach suggested by [14] has obtained the highest precision of 91.00%. Meanwhile, our proposed AWTPSO model obtains higher precision than both previous models, which is 99.99% using the same conditions. Therefore, the proposed AWTPSO model is the best in terms of precision.

The third metric to consider is recall. In a study by [4], they propose an SSK-DDoS system which achieves the highest recall rate of 73.00%. Conversely, [11] suggests a multi-tier model that achieves a recall rate of 28.6%, while [12] introduces the DIDDOS approach with the highest recall rate recorded at 99.91%. In the same manner, the bandwidth control mechanism proposed by [13] has obtained the highest recall of 96.00%, while the hybrid deep learning approach suggested by [14] has obtained the highest recall of 99.00%. Meanwhile, our proposed AWTPSO model obtains a higher recall than both previous models, which is 99.98% using the same conditions. Therefore, the proposed AWTPSO model is best in terms of recall.

The fourth and final metric is the F1 score. According to [4], they suggest an SSK-DDoS system, and the highest F1 score obtained from their system is 83.00%. Meanwhile, the multi-tier model suggested by [11] has obtained the highest F1 score of 39.2% and the DIDDOS approach suggested by [12] has obtained the highest F1 score of 99.87%. The bandwidth control mechanism proposed by [13] has obtained the highest F1 score of 91.00%, and the hybrid deep learning approach suggested by [14] has obtained the highest F1 score of 95.00%. However, our proposed AWTPSO model obtains a higher F1 score than previous models, with a score of 99.99% under the same conditions. Therefore, the proposed AWTPSO model is the best in terms of F1 score.

5. Conclusion

The proposed model presented in this paper offers an effective solution for detecting LDAP-based DRDoS attacks by utilizing an enhanced PSO algorithm based on an adaptive weighted threshold model. Through the utilization of network traffic features and LDAP protocol features, the proposed model successfully identifies attack patterns and dynamically adjusts the threshold value for each feature, thereby enhancing the accuracy of detection. To verify the effectiveness of the AWTPSO model proposed in this study, it was thoroughly tested and validated using the CICDDoS2019 (LDAP sub-dataset) dataset. The experimental results clearly demonstrate that the proposed model outperforms other state-of-the-art techniques, achieving high levels of accuracy, precision, recall, and F1 score. Specifically, the AWTPSO model accurately detects attacks with an impressive detection rate of 99.99%, while effectively maintaining a low false positive rate of 0.01%. Considering these results, the AWTPSO model proposed in this paper presents a promising solution for the detection of LDAP-based DRDoS attacks on enterprise networks. Future work could involve expanding the application of the AWTPSO model to detect other types of DRDoS attacks or integrating it into existing network security systems for real-time detection and prevention of attacks.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

Conceptualization, Riyadh Rahef Nuiaa, Saif Ali Abd Alradha Alsaidi, and Bahaa Kareem Mohammed; methodology, Riyadh Rahef Nuiaa, Ali Hakem Alsaeedi, and Zaid Abdi Alkareem Alyasseri; formal analysis, Selvakumar Manickam, Riyadh Rahef Nuiaa, and Mohammed Abdulridha Hussain; All authors read and approved the final manuscript.

References

[1] I. Sreeram and V. P. K. Vuppala, “HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm”, *Appl. Comput. Informatics*, Vol. 15, No. 1, pp. 59–66, 2019, doi: 10.1016/j.aci.2017.10.003.

[2] D. Kshirsagar and S. Kumar, “A feature reduction based reflected and exploited DDoS attacks detection system”, *J. Ambient Intell. Humaniz. Comput.*, pp. 1–13, Jan. 2021, doi: 10.1007/s12652-021-02907-5.

[3] M. S. Bilkhu, S. Gupta, and V. K. Srivastava,

"Emotion Classification from Facial Expressions Using Cascaded Regression Trees and SVM BT", *Computational Intelligence: Theories, Applications and Future Directions*, Vol. 2, pp. 585–594, 2019.

[4] N. V. Patil, C. R. Krishna, and K. Kumar, "SSK-DDoS: distributed stream processing framework based classification system for DDoS attacks", *Cluster Comput.*, Vol. 25, No. 2, pp. 1355–1372, 2022, doi: 10.1007/s10586-022-03538-x.

[5] L. D. Hooge, M. Verkerken, T. Wauters, F. D. Turck, and B. Volckaert, "Investigating Generalized Performance of Data-Constrained Supervised Machine Learning Models on Novel, Related Samples in Intrusion Detection", *Sensors*, Vol. 23, No. 4, 2023, doi: 10.3390/s23041846.

[6] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, "Deceptive directories and 'vulnerable' logs: A honeypot study of the LDAP and log4j attack landscape", In: *Proc. of 7th IEEE European Symposium on Security and Privacy Workshops*, Euro S and PW 2022, 2022, pp. 442–447. doi: 10.1109/EuroSPW55150.2022.00052.

[7] Mitre CVE, "Ldap vulnerabilities and disclosures", *MITRE*, 2023, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ldap (accessed May 01, 2023).

[8] C. Iwendi, S. U. Rehman, A. R. Javed, S. Khan, and G. Srivastava, "Sustainable security for the internet of things using artificial intelligence architectures", *ACM Trans. Internet Technol.*, Vol. 21, No. 3, pp. 1–22, 2021.

[9] M. A. Ferrag, L. Shu, H. Djallel, and K. K. R. Choo, "Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0", *Electronics*, Vol. 10, No. 11, p. 1257, 2021.

[10] A. Prasad and S. Chandra, "VMFCVD: An Optimized Framework to Combat Volumetric DDoS Attacks using Machine Learning", *Arab. J. Sci. Eng.*, pp. 1–19, 2022.

[11] T. H. Vuong, C. V. N. Thi, and Q. T. Ha, "N-tier machine learning-based architecture for DDoS attack detection", In: *Proc. of Intelligent Information and Database Systems: 13th Asian Conference, ACIIDS 2021, Phuket, Thailand*, Vol. 13, pp. 375–385, 2021.

[12] S. U. Rehman, M. Khaliq, S. I. Imtiaz, A. Rasool, M. Shafiq, A. R. Javed, Z. Jalil, and A. K. Bashir, "Diddos: An approach for detection and identification of distributed denial of service (ddos) cyberattacks using gated recurrent units (gru)", *Futur. Gener. Comput. Syst.*, Vol. 118, pp. 453–466, 2021.

[13] H. A. Alamri and V. Thayananthan, "Bandwidth control mechanism and extreme gradient boosting algorithm for protecting software-defined networks against DDoS attacks", *IEEE Access*, Vol. 8, pp. 194269–194288, 2020.

[14] T. Liu, F. Sabrina, J. J. Jaccard, W. Xu, and Y. Wei, "Artificial intelligence-enabled DDoS detection for blockchain-based smart transport systems", *Sensors*, Vol. 22, No. 1, p. 32, 2022.

[15] W. Ding, C. T. Lin, and W. Pedrycz, "Multiple relevant feature ensemble selection based on multilayer co-evolutionary consensus mapreduce", *IEEE Trans. Cybern.*, Vol. 50, No. 2, pp. 425–439, 2018.

[16] S. M. Hadi, A. H. Alsaeedi, M. I. Dohan, R. R. Nuiaa, S. Manickam, and A. S. D. Alfoudi, "Dynamic Evolving Cauchy Possibilistic Clustering Based on the Self-Similarity Principle (DECS) for Enhancing Intrusion Detection System", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 5, pp. 252–260, 2022, doi: 10.22266/ijies2022.1031.23.

[17] J. Xu, B. Tang, H. He, and H. Man, "Semisupervised feature selection based on relevance and redundancy criteria", *IEEE Trans. Neural Networks Learn. Syst.*, Vol. 28, No. 9, pp. 1974–1984, 2016.

[18] S. Manickam, R. R. Nuiaa, A. H. Alsaeedi, Z. A. A. Alyasseri, M. A. Mohammed, and M. M. Jaber, "An enhanced mechanism for detection of Domain Name System-based distributed reflection denial of service attacks depending on modified metaheuristic algorithms and adaptive thresholding techniques", *IET Networks*, Vol. 11, No. 5, pp. 169–181, 2022.

[19] A. H. Alsaeedi, A. H. Aljanabi, M. E. Manna, A. L. Albukhnefis, and A. L. A. A. H. A. A. H. A. M. E. Manna, "A proactive metaheuristic model for optimizing weights of artificial neural network", *Indones. J. Electr. Eng. Comput. Sci.*, Vol. 20, No. 2, pp. 976–984, 2020, doi: 10.11591/ijeecs.v20.i2.pp976-984.

[20] S. A. Janabi and A. Alkaim, "A novel optimization algorithm (Lion-AYAD) to find optimal DNA protein synthesis", *Egypt. Informatics J.*, Vol. 23, No. 2, pp. 271–290, 2022, doi: https://doi.org/10.1016/j.eij.2022.01.004.

[21] M. A. D. A. Shammary, A. L. Albukhnefis, A. H. Alsaeedi, "Extended particle swarm optimization for feature selection of high-dimensional biomedical data", *Concurr. Comput. Pract. Exp.*, Vol. e6776, No. 34, p. 10, doi:

https://doi.org/10.1002/cpe.6776.
[22] D. A. Shammary, A. L. Albukhnefis, A. H. Alsaeedi, and M. A. Asfoor, "Extended particle swarm optimization for feature selection of high-dimensional biomedical data", *Concurr. Comput. Pract. Exp.*, Vol. 34, No. 10, 2022, doi: 10.1002/cpe.6776.
[23] E. S. P. Krishna and T. Arunkumar, "Hybrid Particle Swarm and Gray Wolf Optimization Algorithm for IoT Intrusion Detection System", *Int. J. Intell. Eng. Syst.*, Vol. 14, No. 4, pp. 66–76, 2021, doi: 10.22266/ijies2021.0831.07.
[24] R. R. Nuiaa, S. Manickam, A. H. Alsaeedi, and E. S. Alomari, "A new proactive feature selection model based on the enhanced optimization algorithms to detect DRDoS attacks", *Int. J. Electr. Comput. Eng.*, Vol. 12, No. 2, 2022.
[25] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", in *2019 International Carnahan Conference on Security Technology (ICCST)*, pp. 1–8, 2019, doi: 10.1109/CCST.2019.8888419.
[26] K. M. Rao, G. Saikrishna, and K. Supriya, "Data preprocessing techniques: emergence and selection towards machine learning models-a practical review using HPA dataset", *Multimed. Tools Appl.*, pp. 1–20, 2023.
[27] D. Singh and B. Singh, "Investigating the impact of data normalization on classification performance", *Appl. Soft Comput.*, Vol. 97, p. 105524, 2020.