GRU-BWFA Classifier for Detecting DDoS Attack within SNMP-MIB Dataset

P Rajasekar (✉ p.rajasekaran537@psnacet.edu.in )
PSNA College of Engineering and Technology  https://orcid.org/0000-0003-1588-1544

V. Magudeeswaran
PSNA College of Engineering and Technology

Research Article

**Keywords:** DDoS attacks, SNMP-MIB dataset, Gated Recurrent Unit-Neural Networks based on Bidirectional weighted average classifier, Enhanced Salp Swarm Optimization (ESSO).

**Posted Date:** December 8th, 2021

**DOI:** https://doi.org/10.21203/rs.3.rs-848205/v1

**License:** ☑️ This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
GRU-BWFA Classifier for Detecting DDoS Attack within SNMP-MIB Dataset

*1P. Rajasekaran, 2V. Magudeeswaran

*1Assistant Professor, Department of ECE, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India.

2Associate Professor, Department of ECE, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India.

*Corresponding Author Mail ID: p.rajasekaran537@psnacet.edu.in

Abstract: With the advancing trends in the field of information technology, the data users were subjected to face different types of attacks. Hence, effective and prompt detection of malicious attacks must be optimized in terms of confidentiality, privacy, availability, and integrity. Accordingly, this research paper provides an effective mechanism for detecting and classifying DDoS attacks such as TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slowloris Slow Post and Brute Force attack, by utilizing machine learning methods within SNMP-MIB dataset. MIB (Management Information Base) is meant for attack classification database linked to the SNMP (Simple Network Management protocol). Three classifiers are considered such as MLP, Random forest, Adaboost to construct the detection model. Significantly, Gated Recurrent Unit Neural Network based on Bidirectional Weighted Feature Averaging (GRU-BWFA) classifier is utilizing as a proposed classifier for high detection rate and accuracy in distinguishing the mentioned DDoS attacks. Feature selection is performed using the Enhanced Salp Swarm Optimization technique to select the optimal features for identifying the attacks. The application of various classifier provides a detailed study on the effectiveness of SNMP-MIB dataset in detecting DDoS attacks. Empirical findings indicate that machine learning methods are highly effective at detecting and classifying the attacks with a higher accuracy rate.

Keywords: DDoS attacks, SNMP-MIB dataset, Gated Recurrent Unit-Neural Networks based on Bidirectional weighted average classifier, Enhanced Salp Swarm Optimization (ESSO).

I. INTRODUCTION

Pervasive computing is a model which indicates a paradigm where it is connected by computing element and sensors linked to all types of everyday objects, which is easily accessible to the users [1]. It is the best example of pervasive computing in automobile networks, which can be implemented as computational elements in automobiles, road infrastructure, and user's equipment interoperated to enhance safety measures even without the user's surveillance. It is termed as 'pervasive' in nature as it brings forth a series of security alarms. Here, the computing elements are pervasive, which can track users' daily routines and raise privacy concerns. Moreover, the rapidly increasing number of devices enlarges the networks, which signifies the opponent have several targets to attack. So it leads to a massive disaster if the network is not secured intensely. Leaving this system unprotected led to the Miraj Botnet attack [1]. Many pervasive computing components are reactive, which performs actions in response according to changes in environmental behavior. The applications are generally attracted in the high-level, complex event in alter to a low-level primitive event generated by sensors. Many types of research are performed to detect the multiple events by aggregating, filtering and combining the first events. There are many machine learning algorithms, and deep learning techniques are implemented to detect and classify network attacks. The neural networks play a significant role in decision-making at the time of an attack and protect the rest of the network by classifying and identifying the characteristic features and distinguishing the type of attack by training the pervasive computing system's defense mechanism effectively.

The main application of pervasive computing is to make life more sophisticated by offering mobile equipment, and digital infrastructure is proficient at providing the distribution of any sort of services within the environment where people socialize, live or work [2]. Besides, it experiences many types of attacks that effective techniques should eliminate. The pervasive system is embedded and participate in demanding services without the explicit knowledge of the user. The working of pervasive computing is done by sharing mutual information, including personal data, even their preferences like surfing in browsers, time spent in social media, sourcing various products, etc. At a particular time, there are many probabilities for third-party attacks in user profiling, suggestions in social network connection and targeted advertising related to the user's search keywords. In the context-based text or reference, the device fails to identify the
trusted domain and does not have centralized control; security chaos occurs.

The pervasive computers act as a game-changer in the health care industries, which throws multiple features to patients such as continuous observation of heart rate, blood pressure, glucose level and so on by connecting with health experts all over the world [3]. There are various types of attacks such as TCP-SYN, UDP flood, ICMP-echo, HTTP flood, Slowloris, Slow post and Brute force attacks is discussed in this paper. The proposed method used to detect and differentiate all the mentioned attacks with high accuracy and reliability [4]. A TCP-SYN attack is a method of denial of service attacks in which a hacker uses the communication protocol of cyberspace, IP, to bombard an objective system with SYN requests to overcome the connection queue and push a strategy to become insensitive to exact demands. An SYN attack is also called an SYN flood, whereas SYN stands for synchronization. UDP flood attack affects the enormous number of user datagram protocol transmitted to the targeted server with the focus of overwhelming the ability of the device to respond and process. The firewall defending the target server can become exhausted as the outcome of UDP flood, affecting Dos to legitimate traffic. An ICMP echo is called a ping flood. The hacker attempts to devastate a targeted device with ICMP echo request packets, causing the target to become unreachable to general traffic. When the attack occurs from multiple devices, it turns into a distributed denial-of-service attack. The HTTP flood exploits the authentic HTTP GET to attack web applications or web servers. It is a volumetric attack, which uses a zombie army to attack the group of computers connected to the internet, which maliciously overrides the system with malware Trojan Horses' assistance. The Slow Loris attack enables a single machine to bring down the webserver of the other device with minimal bandwidth, which impacts unrelated ports and services. It holds many connections to the target web server open and has it as long as possible by establishing the connection by sending a partial request to the target web server. In the Slow Post attack, the hacker sends original HTTP POST headers to a web server. Here the message is transmitted painfully at slow speeds, such as one byte for every 120 seconds. A Brute Force attack is made to crack the username or passwords to identify the hidden web pages or encrypt a text by repeated trial and error method until the correct guess. Even though it is a very traditional method, it remains popular among hackers. Deep learning methods are implemented effectively in recent days to detect network attacks in pervasive computing environments. But the existing techniques are not reliable and efficient in higher dimensional networks. So the proposed method is based on the feature selection and classification of deep learning methods.

DDoS (Distributed Denial of Service) attack is a deliberate attempt for disrupting normal traffic by internet traffic jam or the related networks. Further, these DDoS attacks will be more efficient when utilizing multiple computer systems as an attack source. The DDoS attack requires the attackers to regulate the outline machine networks for an attack. When DDoS attack occurs, the malware is compromised by IoT devices and computers, such that they are transformed to a bot. Hacker will be remotely regulated by bot-groups, namely botnet. Moreover, when a botnet is determined, the attackers control the machines via remote-control by distributing the updated instructions to every bots. The following are the types of DDoS attacks.

**Types of DDoS attacks:**

**TCP SYN Flood** – In this attack, the attackers transmits the TCP SYN packets by utilizing fake IP addresses to the targeted server. The server that has zero knowledge about this attack, receives multiple communication requests. Further, the SYN ACK packet responds each and every attempt from all the open ports.

**UDP Flood** – In this attack, the attackers utilize huge source IP for sending high speed a user datagram protocol (UDP) packets at higher packet rate. Such that, multiple incoming user data protocol packets overwhelmed the target network. Further, this attack absorbs every network resources as well as capacity.

**ICMP ECHO** - This attack is also called ping flood attack, in which the attacker intends to over attack a victim device with ICMP echo pings. For detecting connections as well as connectivity between sender and device, reply messages as well as ICMP echo pings are used as network device. Then the network will be forced to respond similar amount of the reaction packets by overwhelming the victim network with query packets.

**HTTP flood** – This attack uses POST or GET HTTP requests for attacking a web application or web server. This attacks are called volumetric attacks, which utilizes a botnet. Further, these attacks don’t use reflection or spoofing methods, malformed packets, and also they require very less bandwidth when compared to other attacks. All these makes
HTTP flood attack substantially harder for detecting as well as blocking.

**Slowloris attack** - SlowLoris attack is also called, attacks by slow header. Here, the attacker transmits sessions with higher workload requests with different and unexpected IP addresses. These quickly grow, and they never close. This attack results in network or webserver crash.

**Slowpost attack** – The Slowpost attack is known as slow request bodies, this attack is close to slowloris attack, where it submits work load requests for accessing the webservers. This attacker will transmit HTTP header request that defines the contents in post message field. Further, these information are sent for every 2 minutes for filling the message box at 1 byte frequency, the database waits until every message body is completed, later they are rejected.

The major contribution of this study involves,

- For detecting and classifying DDoS attacks such as TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slowloris Slow Post and Brute Force attack, various machine learning methods are considered within SNMP-MIB dataset.
- The feature selection is made by using Enhanced Salp Swarm Optimization. It is used to improve the detection rate of various DDoS attacks by selecting only the optimal features using the wrapper technique. In turn, it increases the accuracy as it is highly dependent on the proposed classifier.
- The proposed classifier used in GRU-NN based on Bidirectional weighted feature averaging namely GRU-BWFA is used to achieve a high prediction rate and classify the DDoS attacks depending on the weights by analyzing the attacks' characteristic features and preventing frequent lags.

The following section II describes the literature review about the pervasive computing associated with various network anomalies. Moreover, several techniques also discussed. Section III elaborated the proposed methodology of GRU based Bidirectional weighted feature averaging. Section IV illustrated the results and discussion of the proposed work. Finally, in section V, the paper is concluded.

### II. REVIEW ON EXISTING WORKS

This section explained the different types of attacks in pervasive computing by various methods implemented in existing research. The benefits of each technique are inferred in the proposed way. The limitations are overcome to improve the performance metrics of our proposed research.

This study proposed the learning ability of detection performance based on deep neural networks by using gated recurrent units. It comprises of neural network with softmax layers and multilayer perceptron. The recurrent neural networks consist of gated units to store central memory units merged with multilayer perceptron to find the network attacks. The KDD dataset is used here for intrusion detection and classification, and it doesn't require any human efforts in feature selection. The process is more suitable in the RNN memory unit than LSTM in intrusion detection. The advantage of this method, such as time consumption and performance metrics, are attractive. Still, it should be more updated to be applied in real-time environments as suggested by network experts since it is only reliable up to a particular extent [5].

Further, this research explained the capability of learning from the previous attacks by supervised intrusion detection using recurrent neural networks. The developed Learning is based on fast learning networks based on particle swarm optimization applied in the KDD dataset. It is processed by comparing with a wide range of existing algorithm for training the extreme machine learning and Fast learning classifiers. The calculated performance metrics overcome various algorithms. So the PSO process is inferred, and advantages can be considered for our proposed work [6].

This study proposed research to achieve network security by managing the traffic flow to detect malicious host attacks. So many techniques are adapted for controlling cyber-attack. The suggested paper identifies the malware attack based on the characteristics when sending the SYN packets. The matrix method is used to transform SYN packets to an input visual image for neural networks. The image comprises distinctive features of the host's behavioural characteristics, and the convolutional neural network effectively segregates the malevolent host from the general ones. The evaluation of real-world traffic showed a detection accuracy of 98%. Still, it only detects at the time of sending the packets of SYN. It isn't able to identify any other malware attack. So it is not efficient in distinguishing different types of attack and cannot be applied in a real-time system [7]. This paper deliberated the detection of known and unknown attacks by a defence mechanism that prevents the counterfeit packets from the victim's
destiny point. It enables only the original packets to pass through by training the dataset with neural networks. It focuses on the detection of known attacks in the higher volume of traffic without any packet drop. The dataset is trained, deployed and tested in physical circumstances as a desperate to the simulators. It is introduced to lower the attack's impact and strength before it reaches the victim by the intrusion detection system. The evaluated method is analyzed by computing the performance metrics. But this method cannot differentiate the type of attack and cannot be implied in real-time environments [8].

This research explained the attacks and impacts on the advanced paradigms in pervasive computing. This method revealed the detection model in pervasive computing architecture to closely resemble human decision-making by using neural networks. Here the Apriori algorithm is used to extract the behavioural sequences adapted from the users at network interactions. Then, the Naïve classifier is implemented for the final decision to check the trustworthiness of the network. The neural network is used in the detection of intrusion. Still, it does not achieve a reliable metric when applied in the sizeable dimensional dataset and cannot classify many types of network attacks [9]. This study explained the intrusion detection system to correct the abnormalities in pervasive environments. It is a traditional method that manages the security of the node and network and always is cautious on the network security and isolates the affected node from the rest of the system [10]. This suggested method implemented authentication methods to develop the user profile, enabling flexible detection and analysis to avoid updating the general profile database. Processing network clusters' orchestration performs the investigation methods to explore the audit information from IDS. In this method, three phases are completed, such as the initialization phase, the detection phase and the isolation phase. The Georgia Tech Network Simulator is used for the simulation process, which is updated to the current environment's demands with many machine learning and deep learning concepts in pervasive computing [11].

This study explained the intrusion detection method to find malicious detection by improvised convolutional neural networks. The traffic data is characterized and preprocessed by optimizing the network parameters in extracting the sample features using a stochastic gradient descent algorithm in the convergence model. The sample test and simulation result are used to test the existing system's performance metrics in the KDD dataset. But the network flow has given a minimum performance in detecting the malicious attack at the time of traffic management in the wireless network system [12]. This paper deliberated the extensive analysis of deep learning methods for intrusion detection in networks [13]. This method used the Restricted Boltzmann machine based on clusters. The supervised machine learning approach is based on adaptively supervised and clustered hybrid ID. The Restricted Boltzmann device comprises two layers, hidden and visible, for the weight selection of the cluster head in the pseudo-code, which is used for cybersecurity. Even though it shows high-performance outcomes, it cannot be applied in large scale networks [14].

This research described joint intrusion learning on pervasive systems by detecting the different intrusion sequences simultaneously. The K-neighborhood method is used for grid-based clustering for detecting the occurrence or presence of interferences. The joint learning approach showed the performance metrics with minimum FPR by conducting experiments using Zigbee. But it should be improved by using the collative detection efforts among the multiple pairs of transmitter-receiver [15]. This study explained to overcome the security challenges in ubiquitous healthcare systems. The pervasive computing system and universal are similar involves computational, complicated and expensive task in simultaneous execution of the algorithm. It is responsible for characterizing any attack in the networks and computing the physical parameters of attacks that can be used for future research. In this method, the collective computing capability with wireless connected local mobile networking grid and various sensors. Here, the sensor plays a data provider by offloading the task, which executes a different intensive algorithm. The raw data is sent via zig bee to manage the elastic data pool. So if any attack exists, the computational load on the node is decreased since the parallelism of data is performed. The vital signs are collected and processed for contextual information, which is used for patient-centric decision-making and can be further used for research application by converting it as a dataset [16].

III. Proposed Methodology

The overview of the proposed method is shown in Fig.1, and a brief explanation is given in the below section. The preprocessing is applied to remove the noises in the data, fed for feature selection by using the Enhanced Salp Swarm Optimization technique to find the optimal features to detect DDoS attacks in the pervasive computing. Then, GRU-NN based Bidirectional weighted feature averaging namely
GRU-BWFA is used as a classifier to differentiate various types of DDoS attacks such as TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slowloris, Slow Post and Brute Force. It is made by analyzing the characteristic features and weighted average of the attack with the trained SNMP-MIB dataset.

Fig.1 Architecture- GRU-BWFA classifier for Detecting D-DoS attacks

3.1. Dataset Description

For detecting the DDoS attack using GRU-BWFA classifier, SMP-MIB dataset is utilized [5]. MIB (Management Information Base) is meant for attack classification database linked to the SNMP (Simple Network Management protocol). The major reason of utilizing this specific dataset is that it comprised with unique records, realistic network traffic simulates and 34 MIB variable records are presented. The attacks are obtained in 6 DoS attack forms such as (TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slowloris, Slow Post) and Brute Force attacks. In Table 1, the MIB dataset and cases which is recorded are described and the dataset comprised with 4998 MIB records [16]. Further, the procedure of collecting MIBs of SNMP is demonstrated as below in Fig. 2.

Table 1: Number of generated records based on type of traffic [5]

| S.No. | Number of records | Traffic type   |
|-------|-------------------|---------------|
| 1.    | 600               | Normal        |
| 2.    | 960               | TCP-SYN       |
| 3.    | 773               | UDP-flood     |
| 4.    | 632               | ICMP-ECHO     |
| 5.    | 573               | HTTP-flood    |
| 6.    | 780               | Slow loris    |
| 7.    | 480               | Slow post     |
| 8.    | 200               | Brute Force   |

3.2. Preprocessing

Whenever the information is collected from varied resources noises or any data errors, missing or repetitive values can be occurred. The format may also be not feasible to feed into an algorithm for analysis, so it should be appropriately formatted to understand machine learning algorithm or deep learning techniques that should be executed in the proposed method. The preprocessing process using filtering techniques to eliminate the errors and noise data.

3.3. Data encoding

Once the preprocessing is completed, the data is encoded for better clarity and security purposes. The encoder is used to encode every string into numerical values into binary formats. The data loss, data threat and hack are avoided, and thus, the data can be transmitted in a secured packet to the destination point. It also removes the preprocessing glitches since it is completely purified and connected before it is fed into the optimization algorithm.

3.4. Enhanced Salp Swarm Optimization (ESSO) for Feature Selection

The general Salp Swarm Algorithm undergoes the difficulty of population diversity and trapped into local optima. The proposed algorithm is implemented to overcome the limitations by making two strategies in the usual Salp Swarm Optimization algorithm [17]. The first strategy is implementing the Opposition Based Learning (OBL) method at the initializing phase of SSO to enhance the population diversity [18]. The second strategy is implemented to develop a local search algorithm applied at the ending step of SSO. It is used to increase the SSO utilization and prevent it from being stuck at local optima. So the Enhanced Salp Swarm Optimization is used to
resolve the feature detection and choose the optimum subset of features by wrapper technique.

Opposite based Learning is an optimization method used to increase the quality of commenced population solution by the diversity of solutions. It works by searching in both directions in space search. The two approaches involve one of the original solutions is symbolized by its opposite solution, which is used to take the fittest answer from all the generated keys. The Local Search Algorithm is used at the end of every iteration in Salp Swarm Optimization to improve the obtained best solution, E. Initially, the LSA executes by storing the value of obtained best solution received from SSO. At the final iteration of SSO, it is stored as a temporary variable.

The proposed Enhanced Salp Swarm Optimization works with GRU-NN based Bidirectional Weighted Feature Averaging classifier by wrapper function for feature selection. It is implemented on the training dataset to compute the feature subset for training the proposed classifier. The binary values 1 and 0 are performed to choose the unselected and selected features. The value 1 represents the selected feature mentioned in the given label or index, whereas 0 indicates the unselected elements in the title or index.

The following equations describes the enhanced Salp swarm optimization for feature selection,

\[
(y_r) = t_a + v_a - y_i \quad \text{where} \quad r = 1, 2, \ldots G
\]

(1)

\[
E_i = 2d - (\frac{4r}{T})^2
\]

(2)

\[
y_i^1 = \begin{cases} 
E_i + e_1 ((v_a - t_a)e_2 + t_a) e_3 & \text{if } \{E_i + e_1 ((v_a - t_a)e_2 + t_a) e_3 \} \geq 0.5 \\
E_i + e_1 ((v_a - t_a)e_2 + t_a) e_3 & \text{if } \{E_i + e_1 ((v_a - t_a)e_2 + t_a) e_3 \} < 0.5 
\end{cases}
\]

(3)

\[
y'_i = \frac{1}{2} (y^i + y'^{i-1})
\]

(4)

Where \( y'_i \) position of ith followers salp in the jth dimension

\( E_i \) position of food source in i-th dimension

\( v_a \) denotes upper bound of jth dimension

\( t_a \) denotes lower bound of jth dimension

The initialization of ESSO is made by a randomly generated number of salps based on the population's size. The developed solution comprises a subset that is randomly chosen from the entire set of features. The OBL is applied to find the opposite solution of every obtained answer to step 1. The suitable fitness value ‘E’ is obtained, which also signifies the lower classification accuracy error. Each position of a slap is updated by choosing the leader of the salp chain by eqn 3. The fitness value of all solved slap is determined to find the ‘E’ best solution. LSA is implemented in the end phase of ‘E’ to find the best solution; then, the iteration is repeated thrice or more. The best solution is determined with ESSO, signifying the suitable subset features to be selected and applied.

**Feature Scaling**

It is also a standardization method similar to preprocessing executed in independent features or variables of data to normalize within an applicable range. It also helps in speed up the computation in the algorithm. Here, the standard scalar is used to scale
the obtained data, which should be further used as input for the classifier.

### 3.5. Gated Recurrent Unit – Neural Networks based new Bidirectional Weighted Feature Averaging (GRU-BWFA)

The GRU-NN based on bidirectional weighted feature averaging is used to train, test, and classify the data. The Gated Recurrent Units is considered a modest version of LSTM [19]. Here two gates are involved as a reset gate which alters the integration of new input with preceding memory. Another is the update gate which controls the preservation of the last memory that is implemented. The hidden units of Gated Recurrent Units are represented as transition functions. The integrated bi-directionality of the recurrent method can enhance the proposed design’s flexibility and capability. Gated Recurrent Unit GRUs are termed as gating mechanism in recurrent neural networks. Like long short-term memory LSTM with forget gate, it consists of few parameters compared to LSTM, which lacks an output gate. Hence, the new enhanced Salp Swarm Optimization method has solved the population diversity, and local optima trap issues. Using two approaches is Opposition Based Learning (OBL) and the local search algorithm. So the Enhanced Salp Swarm Optimization is to select the optimum subset with the wrapper technique’s help. The wrapper function utilizes the GRU-NN based Bidirectional Weighted Feature Averaging classifier employed with enhanced SSO (ESSO). The GRU-NN architecture shown in following fig.3.

**Fig.3.** GRU-BWFA Architecture

Due to additional weight matrices in LSTM, the computational complexity increased. Thus by introducing GRU the complexity is reduced by joining the input and LSTM forget gate into single update gate. The hidden and cell states are combined into single hidden state. The equations are expressed as,

\[ V = \text{transformation matrix} \ b = \text{bias value} \]

\[ g_k = \varphi(V^g y_k + S^g g_{k-1} + a^g) \]  \hspace{1cm} (5)

\[ y_k = \text{current input} \quad g_{k-1} = \text{previous activation} \]

\[ s_k = \delta(V^s y_k + S^s g_{k-1} + a^s) \]  \hspace{1cm} (6)

\[ z_k = \{ \delta(V^z y_k + S^z g_{k-1} + a^z) \} \]  \hspace{1cm} (7)

\[ \bar{g}_k = \{ \delta(V g y_k + S g (S g g - 1) + a g) \} \]  \hspace{1cm} (8)

\[ g_k = \{ z k \odot g k - 1 + (1 - z k) \odot \bar{g}_k \} \]  \hspace{1cm} (9)

\[ s_k, z_k \text{ and } g_k \text{ are the update, reset and hidden states correspondingly.} \]

**3.5.1. Bidirectional GRU with weighted feature averaging**

The bidirectional recurrent process operates in two directions, such as backward and forward directions includes two hidden layers. The function of the hidden layer is to capture the past and future context together. The property of bi-directional method can emphasize the memory at initial and final stages of input raw time-series. The complete hidden component is represented at the final step is the output concatenated vector of the forward and backward process, which can be considered as the raw sensor signal. Moreover, the information in the middle range of sequence that might be lost in the bidirectional gated recurrent unit. Hence the weighted feature average is to give another view of selected features which indicates the novelty of this study. The equations are expressed as,

\[ g_L = \bar{g}_L \odot \bar{g}_L \]  \hspace{1cm} (12)

\[ g_L \text{ rept hidden elements} \]
The obtained value predicts the type of DDoS attacks such as TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slow Loris, Slow Post and Brute Force attacks. The experimental values are collected and compared with the attack based on their obtained weighted average values. Analyzing the characteristics of attack and computing the weighted average and corresponding with estimated values can be detected and classified the types of attacks using the well-trained SNMP-MIB dataset.

## IV. RESULTS AND DISCUSSION

The experimental analysis is performed by using the SNMP-MIB dataset and compared with various existing studies. The value of accuracy, precision, recall and F-Measure is calculated for different types of attacks in the proposed method. In detecting an attack, GRU-BWFA classifier gives a high recognition rate and provides increased accuracy in classifying different types of DDoS attacks [20].

### 4.1. Performance metrics

The performance metrics such as accuracy, detection rate, precision, recall and the proposed method are calculated and explained briefly in the upcoming section, and obtained results are compared with the existing techniques to prove the proposed approach's efficacy.

**Accuracy:**

Accuracy is computed to analyze the performance and efficiency of the proposed system. It is calculated by finding the ratio of summation of true positive and real negative to the overview of total positive and negative values.

**Detection rate:**
Detection rate is defined as calculating the total number of correctly detected attack by the total number of mentioned attacks.

**Precision:**

Precision is a significant performance metrics evaluated to find the positively predicted attacks to the total number of a mixture of attacks along with probable values of correct or wrong identification attacks.

**Recall:**

The recall is referred to as the sensitivity of a proposed method: the ratio of the total quantity of related instances that are truly associated.

**F-Measure:**

F-Measure is used to test the proposed technique's accuracy by computing the weighted harmonic mean of tested standards of precision and recall.

The performance metrics of the proposed method is high in detection and classification of various types of attacks is explained in table.1, and the comparison of multiple attacks is illustrated in fig.2.

| Performance metrics | TCP-SYN | UDP Flood | ICMP ECHO | HTTP flood | Slow Loris | Slow post | Brute force |
|---------------------|---------|-----------|-----------|------------|------------|-----------|-------------|
| Accuracy            | 1       | 1         | 1         | 0.9        | 0.98       | 0.98      | 1           |
| Precision           | 1       | 1         | 0.98      | 1          | 0          | 1         | 1           |
| Recall              | 1       | 1         | 1         | 0.98       | 0.95       | 0.9       | 0.91        |
| F-Measure           | 1       | 1         | 1         | 0.92       | 0.9        | 0.9       | 1           |

From the table.2, it is shown that the value of the performance metrics in the detection of DDoS attacks such as TCP-SYN, UDP flood, ICMP-echo, HTTP flood, Slow Loris, Slow Post and Brute force. The proposed techniques are efficient in detecting the attacks since higher accuracy is obtained. But in the slow post case, the precision value is higher where it sees various types of malware in the system. Since the value of precision is high in identifying the different types of attack, and thus the loss in the network is avoided. The recall value is high in TCP-SYN, UDP flood, ICMP-echo and Brute force, which can classify the affected systems precisely. But in HTTP flood, Slow Loris and Slow post, recall is low, but the F-measure is high, which at least can identify the various attacks in the system.

The proposed method's performance metrics in the detection and classification of DDoS attacks are shown in fig.4. From fig.4, it is shown that in the detection of TCP-SYN, UDP-flood and ICMP-echo, the values of accuracy, precision, recall and F-measure are high, which signifies the correct classification of attacks that can be used to get the optimal solution for the recovery of the network. In the detection of HTTP flood, the value of precision is high compared to other performance metrics, which at least indicate the presence of attack in the system. There is the only average value of accuracy, f-measure and recall in slow Loris and slow post, which identifies the system's attack.

From fig.5, the comparison of accuracy by the other existing scenario and the proposed method is shown. The proposed method, GRU-BWFA, outperforms the existing process by achieving an efficiency of 99.99%.
From fig.6, the comparison of detection rate by the various existing plan and the proposed method is shown. The proposed method outperforms the existing process by achieving an accuracy of 99.9%. The existing fuzzy rule method has detection rate of 93.99%. If the detection rate is minimum, the system may fail to identify the attack spontaneously, and system failure is possible. Thus detection rate helps in the classification of various types of attacks to take a suitable solution as soon as possible to restore the network's working. Since GRU-BWFA gave a high value of detection rate.

The confusion matrix for the proposed and existing system is explained in fig.7, which comprises the total number of instances, regular tariffs test and up to routine tariff tests. Table 3 and 4 shows that the GRU-BWFA resulted in higher precision and F-measure value than the existing system such as Lazy, zblk, trees, Random forest and meta. Random committee. Thus, the GRU-BWFA is secure against various attack.

### Table 3 Comparative analysis- F-measure value for all attributes [23]

| Methods         | Normal | ICMP | ECHO  | TCP-SYN | UDP Flood | HTTP Flood | Slow Loris | Slow post | Brute force |
|-----------------|--------|------|-------|--------|-----------|------------|------------|-----------|-------------|
| Lazy.lbk        | 100    | 99.89| 99.89 | 99.89  | 99.89     | 99.85      | 100        | 100       | 100         |
| Meta.Random committee | 99.89 | 99.85| 100   | 99.85  | 99.89     | 99.89      | 100        | 100       | 100         |
| Trees. Random Forest | 99.85 | 99.89| 99.89 | 99.89  | 99.85     | 99.85      | 100        | 100       | 100         |
| GRU-BWFA        | 99.98  | 99.98| 99.98 | 99.98  | 99.85     | 100        | 100        | 100       | 100         |

### Table 4 Comparative Analysis- Precision for all attributes [23]

| Methods         | Normal | ICMP | ECHO  | TCP-SYN | UDP Flood | HTTP Flood | Slow Loris | Slow post | Brute force |
|-----------------|--------|------|-------|--------|-----------|------------|------------|-----------|-------------|
| GRU-BWFA        | 99.98  | 99.98| 99.98 | 99.98  | 99.85     | 100        | 100        | 100       | 100         |
Random forest and MLP in all kinds of attacks except for MLP classifier in the Brute attack where its efficacy was less effective compared to other attacks. Also, the Ada Boost MI classifier has the minimal outcome for the UDP flood attacks.

Table 5 and fig8 revealed the accuracy results are higher based on all the attack types for GRU-BWFA compared with adaboost, random forest and MLP.

| Algorithm       | Accuracy |
|-----------------|----------|
| Ada Boost MI    | 99.6     |
| Random Forest   | 99.93    |
| MLP             | 98.86    |
| GRU-BWFA        | 99.97    |

**Table 5 Comparison of accuracy for existing and proposed system [24]**

Figure 9 displays that precision outcome are higher for the other existing classifiers such as Adaboost, Random forest, and MLP classifier in the Brute attack where its efficacy was less effective compared to other attacks. Also, the Ada Boost MI classifier has the minimal outcome for the UDP flood attacks.

**Fig. 8. Comparative analysis of accuracy for GRU-BWFA and Machine learning models**

**Fig 9: Precision comparison**

| Algorithm       | Normal | ICMP - ECHO | TCP - SYN | UDP Flood | HTTP Flood | Slowloris | Slowpost | Brute Force |
|-----------------|--------|-------------|-----------|-----------|------------|-----------|----------|-------------|
| Ada Boost MI    | 100    | 100         | 100       | 97.85     | 100        | 100       | 100      | 100         |
| Random Forest   | 100    | 100         | 100       | 99.86     | 100        | 100       | 100      | 100         |
| MLP             | 100    | 99.56       | 99.56     | 99.46     | 100        | 100       | 99.79    | 88          |
| GRU-BWFA        | 100    | 99.89       | 99.95     | 99.93     | 100        | 100       | 100      | 100         |
The result in fig.10 represent that the three classifiers attained very high result detecting the normal traffic records, as well as the slowloris and slowpost attack records in the testing set with high recall values of 100. From the result, random forest and Ada Boost classifiers outperform in detecting many types of attacks by random forest which also attained high performance for attack detection. More specifically, the proposed classifier GRU-BWFA achieved the best recall outcomes for all types of attack.

![Fig. 10: Recall comparison](image)

Table: 7 Comparative analysis of recall for GRU-BWFA and machine learning algorithms

| Algorithm       | Normal | ICMP - ECHO | TCP - SYN | UDP Flood | HTTP Flood | Slowloris | Slowpost | Brute Force |
|-----------------|--------|-------------|-----------|-----------|------------|-----------|----------|-------------|
| Ada Boost MI    | 100    | 99.61       | 98.45     | 100       | 100        | 100       | 100      | 100         |
| Random Forest   | 100    | 99.61       | 100       | 100       | 100        | 100       | 100      | 100         |
| MLP             | 100    | 95.5        | 100       | 99.54     | 97.85      | 100       | 100      | 97.32       |
| GRU-BWFA        | 100    | 99.89       | 100       | 100       | 100        | 100       | 100      | 100         |

The above table 7 shows the recall comparison for various machine learning models and GRU-BWFA model which has slight changes in the values. The more number of attacks has been detected as shown in results.

Table 8: Comparative Analysis of various machine learning algorithms [25] with GRU-BWFA within SNMP-MIB dataset

| DDoS detection measures | SNMP MIB’s under consideration                                                                 | Accuracy (%) |
|-------------------------|------------------------------------------------------------------------------------------------|--------------|
| SVM                     | tcpAttemptFails, tcpOutRsts                                                                      | 97.7         |
| C4.5 decision tree      | tcpAttemptFails, tcpOutRsts                                                                      | 99.1         |
| HMM based Viterbi       | ifnOctets, ifoutDiscards, ifnNUcastPkts, ifOutUcastPkts, ifOutNUcastPkt                           | 99.1         |
| Kolmogorov Smirnov Test | tcpPassiveOpens, tcpAttemptFails, tcpInSegs, tcpOutSegs                                         | 98           |
The above table 8 shows the performance comparison of GRU-BWFA for the SNMP-MIB dataset with the various existing machine learning models. The results show that GRU-BWFA shows superior performance as its accuracy value is 100% compared with the SVM, C4.5 decision tree, HMM based Viterbi algorithm, Kolmogorov Smirnov Test and gradient descent models.

V. CONCLUSION

In Information technology, DDoS plays a crucial role in affecting the network’s overall performance. Even though there are many existing methods in detecting DDoS, there is no reliability in classifying the types of attacks such as TCP-SYN, UDP flood, ICMP-echo, HTTP flood, Slow Loris, Slow Post and Brute force, which may lead to false identification and, in turn, affects its restoring capacity and originality of the network. So the proposed technique with Enhanced Salp Swarm Optimization for feature selection is used to select the SNMP-MIB dataset’s optimal features. Once the detection of attack is made, the appropriate classification is made using the proposed classifier, Gated Recurrent Unit Neural Network, based on Bidirectional weighted feature averaging (GRU-BWF A). From the results it shows that the performance of each classifier varies where the accuracy rate varied among three classifiers. The proposed system GRU-BWFA attained the highest accuracy rate of 99.9% accuracy and detection rate proved that the proposed method outperforms the existing techniques to classify and detect various attacks from SNMP-MIB dataset. Thus the system is restored effectively in minimal time.

VI. Declarations

Funding

This research work was not funded by any organization/institute/agency.

Conflicts of Interest

I confirm that this work is original and has either not been published elsewhere, or is currently under consideration for publication elsewhere. None of the authors have any competing interests in the manuscript.

Data Availability

1. https://doi.org/10.1109/iisa.2018.8633687
2. https://d1wqtxslxze7.cloudfront.net/51132818/122_Paper_310816214_IICSIS_Camera_Ready_pp_1162-1185-with-cover-page-v2.pdf?Expires=1629891546&Signature=E-XOLhFp8RkQnJHtr1xvwPNKJ7piQanBS1Nxa2ZgDHf11aywY-uJrJrbCtw0sBnkkaSat7NqZhZgncSyoMgRxMzIKPL1HQqTEqwHuvd0KD9mEgUb-5LijshWDbdxwST-sPeVChxB513LrtmVo1Hx6eXQYTIzQS1npnWsxLS89-uOnIPCzIgL7vW4k9BVu0Yw3kZ8a90BoezQ6YaMw7vqimM6o2YIVSzi5jMV5Zs2GpEVXvKcBSybWXjldP2TE-%M-JZdusr4VMFAHtufd404E9cfp3-j-un3pSKn-6kTAMIxxeUMSPVrmw1F1NY0TuHdKgO1wBzXw_&Key-Pair-Id=APKAJLOHF5GS1RBV4Z4A
3. https://doi.org/10.17485/iijst/2017/v10i3/110619
4. https://doi.org/10.1016/j.bspc.2017.03.018
5. https://doi.org/10.1109/access.2018.2867564
6. https://doi.org/10.1109/access.2018.2820092
7. https://doi.org/10.1109/isncc.2018.8530964
8. https://doi.org/10.1016/j.neucom.2015.04.101
9. https://doi.org/10.1007/s00500-016-2183-1
10. https://doi.org/10.1109/3pgcic.2015.94
11. https://doi.org/10.1109/access.2019.2917299
12. https://doi.org/10.1109/lcnw.2018.862859
13. https://doi.org/10.1109/het.2019.2901797
14. https://doi.org/10.1016/j.access.2017.278544
15. https://doi.org/10.1109/936978-0-12-819361-7.00001-4
16. https://doi.org/10.1016/j.cose.2016.06.005
Code availability

N\A

Authors' contributions

I Am P. Rajasekaran Hereby State That The Manuscript Title Entitled “GRU-BWFA Classifier for Detecting DDoS Attack within SNMP-MIB Dataset” Submitted To The Wireless Personal Communications, I Confirm That This Work Is Original And Has Not Been Published Elsewhere, Nor Is It Currently Under Consideration For Publication Elsewhere. And I Am Assistant Professor In the Department of ECE, PSNA College of Engineering and Technology, and Dindigul.

I’m the corresponding author of our paper, my contribution work on this paper is to Writing, developing, and reviewing the content of the manuscript. And my co-author V. Magudeeswaran works were to cite the figure, table and references. We are the entire contributors of our paper. And no other third party people are not involved in this paper.

Ethics approval

No animals or human participants are involved in this research work.

Informed consent

I confirm that any participants (or their guardians if unable to give informed consent, or next of kin, if deceased) who may be identifiable through the manuscript (such as a case report), have been given an opportunity to review the final manuscript and have provided written consent to publish.

REFERENCES

[1] N. Papageorgiou, D. Apostolou, Y. Verginadis, A. Tsagkaropoulos, and G. Mentzas, "A situation detection mechanism for pervasive computing infrastructures," in 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), 2018, pp. 1-8.

[2] M. Al-Kasassbeh, G. Al-Naymat, and E. Al-Hawari, "Towards generating realistic SNMP-MIB dataset for network anomaly detection," International Journal of Computer Science and Information Security, vol. 14, p. 1162, 2016.

[3] P. Sarkar and D. Sinha, "Application on pervasive computing in healthcare—a review," Indian Journal of Science and Technology, vol. 10, 2017.

[4] C. M. Ionescu and D. Copot, "Monitoring respiratory impedance by wearable sensor device: Protocol and methodology," Biomedical Signal Processing and Control, vol. 36, pp. 57-62, 2017.

[5] C. Xu, J. Shen, X. Du, and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," IEEE Access, vol. 6, pp. 48697-48707, 2018.

[6] M. H. Ali, B. A. D. Al Mohammed, A. Ismail, and M. F. Zolkipli, "A new intrusion detection system based on fast learning network and particle swarm optimization," IEEE Access, vol. 6, pp. 20255-20261, 2018.

[7] R. Nakamura, Y. Sekiya, D. Miyamoto, K. Okada, and T. Ishihara, "Malicious host detection by imaging SYN packets and a neural network," in 2018 International Symposium on Networks, Computers and Communications (ISNCC), 2018, pp. 1-4.

[8] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS
attacks using Artificial Neural Networks," Neurocomputing, vol. 172, pp. 385-393, 2016.

[9] G. D'Angelo, S. Rampone, and F. Palmieri, "Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification," Soft Computing, vol. 21, pp. 6297-6315, 2017.

[10] G. D'Angelo, S. Rampone, and F. Palmieri, "An artificial intelligence-based trust model for pervasive computing," in 2015 10th international conference on P2p, parallel, grid, cloud and internet computing (3pgcic), 2015, pp. 701-706.

[11] H. Yang and F. Wang, "Wireless network intrusion detection based on improved convolutional neural network," IEEE Access, vol. 7, pp. 64366-64374, 2019.

[12] M. Abedin, K. N. E. A. Siddiquee, M. Bhuyan, R. Karim, M. S. Hossain, and K. Andersson, "Performance analysis of anomaly based network intrusion detection systems," in 43nd IEEE Conference on Local Computer Networks Workshops (LCN Workshops), Chicago, October 1-4, 2018, 2018, pp. 1-7.

[13] S. Otoum, B. Kantarci, and H. T. Moutfah, "On the feasibility of deep learning in sensor network intrusion detection," IEEE Networking Letters, vol. 1, pp. 68-71, 2019.

[14] J. Lv, D. Man, W. Yang, X. Du, and M. Yu, "Robust WLAN-based indoor intrusion detection using PHY layer information," IEEE Access, vol. 6, pp. 30117-30127, 2017.

[15] P. Mukherjee and A. Mukherjee, "Advanced processing techniques and secure architecture for sensor networks in ubiquitous healthcare systems," in Sensors for Health Monitoring, ed: Elsevier, 2019, pp. 3-29.

[16] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," Computers & Security, vol. 86, pp. 147-167, 2019.

[17] S. Dutta, S. Ghatak, A. K. Das, M. Gupta, and S. Dasgupta, "Feature selection-based clustering on micro-blogging data," in Computational Intelligence in Data Mining, ed: Springer, 2019, pp. 885-895.

[18] J. L. Esquinas-Requena, S. Lozoya-Moreno, I. García-Nogueras, P. Atienza-Núñez, P. M. Sánchez-Jurado, and P. Abizanda, "La anemia aumenta el riesgo de mortalidad debido a fragilidad y discapacidad en mayores: Estudio FRADEA," Atención Primaria, vol. 52, pp. 452-461, 2020.

[19] Y. Xu, Q. Kong, Q. Huang, W. Wang, and M. D. Plumbley, "Convolutional gated recurrent neural network incorporating spatial features for audio tagging," in 2017 International Joint Conference on Neural Networks (IJCNN), 2017, pp. 3461-3466.

[20] M. Alkasassbeh, "A novel hybrid method for network anomaly detection based on traffic prediction and change point detection," arXiv preprint arXiv:1801.05309, 2018.

[21] S. Alhaidari, A. Alharbi, M. Alshaikhsaleh, M. Zohdy, and D. Debnath, "Network traffic anomaly detection based on Viterbi algorithm using SNMP MIB data," in Proceedings of the 2019 3rd International Conference on Information System and Data Mining, 2019, pp. 92-97.

[22] M. Almseidin, M. Alkasassbeh, and S. Kovacs, "Fuzzy rule interpolation and snmp-mib for emerging network abnormality," arXiv preprint arXiv:1811.08954, 2018.

[23] G. Al-Naymat, A. Hambouz, and M. Al-Kasassbeh, "Evaluating the Impact of Feature Selection Methods on SNMP-MIB Interface Parameters to Accurately Detect Network Anomalies," in 2019 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2019, pp. 1-6.

[24] G. Al-Naymat, M. Al-Kasassbeh, and E. Al-Hawari, "Exploiting snmp-mib data to detect network anomalies using machine learning techniques," in Proceedings of SAI Intelligent Systems Conference, 2018, pp. 991-1004.

[25] G. Rajakumaran, N. Venkataraman, and R. R. Mukkamala, "Denial of Service Attack Prediction Using Gradient Descent Algorithm," SN Computer Science, vol. 1, pp. 1-8, 2020.