DETECTION OF COMPUTER VIRUSES USING WELM_BFO
Ankur Singh Bist*
*Computer Engineering K.I.E.T, Ghaziabad

ABSTRACT
Computer viruses are big threat for our society. The expansion of various new viruses of varying forms make the
prevention quite tuff. Here we proposed WELM_BFO to detect computer viruses. The proposed method efficiently
detects static and nature changing viruses

KEYWORDS: Viruses, WELM_BFO.

INTRODUCTION
There are various processes that have been used in the direction of classification of computer viruses from normal
files that will finally lead to virus detection. Machine learning techniques are widely used in this direction. As statistics
says that the attacks of malicious codes are increasing day by day so there is requirement of strong techniques that can
be used for their detection. Malicious code designers use lot of techniques that are difficult to analyse and detect. The
static methods also seems not to work in the case where every time there are rapid dynamicity from attacker side so
now a days main focus is going on towards the methods that are dynamic and are able to detect zero day computer
viruses [1].

The rise in the malicious threats like computer viruses activities are required to be handled and observed strongly to
make certain defence that can stand as a saviour of security domain. Other types of malware are:

1. Worms
2. Trojan horse
3. Botnets
4. Adware
5. Spyware

The mutating behaviour of metamorphic viruses is due to their adoption of code obfuscation techniques like dead
code insertion, Variable Renaming, Break and join transformation. Figure 1 shows the assembly file of the virus code.
Computer viruses like polymorphic viruses and metamorphic viruses use more efficient techniques for their evolution
so it is required to use strong models for understanding their evolution and then apply detection followed by the
process of removal. Code Emulation is one of the strongest ways to analyze computer viruses but the anti-emulation
activities made by virus designers are also active [4] [5] [6] [7] [8].

EXTREME LEARNING MACHINE
Extreme Learning Machine (ELM) [1] is based on least square solution and was originally proposed for single hidden
layer feed-forward network. The advantage of this is, rather than tuning of all the parameters here, hidden neurons
and input weight, are chosen randomly. Here, hidden nodes may be sigmoid additive nodes or Gaussian kernel nodes. Hidden node parameters are randomly taken and output node parameter is calculated using Moore-Penrose inverse. This algorithm is thousand times faster than past learning methods such as, back propagation and also reaches the smallest training error. Due to these features, generalization performance of this algorithm is also good. We have given data \((x_p, t_p)\) for \(N\) random different samples where, \(x_p=[x_{p1, x_{p2}, \ldots , x_{pn}}] \in \mathbb{R}^n\) and \(t_p=[t_{p1, t_{p2}, \ldots , t_{pm}}] \in \mathbb{R}^m\).

Activation function \(g(x)\) with \(L\) hidden nodes is defined as

\[
\beta_p \cdot g_p(x_q) = \beta_p \cdot g(w_p \cdot x_q + b_p) = o_q \quad \text{for} \quad q=1,2,3,\ldots,N
\]

Where \(w_p=[w_{p1, w_{p2}, \ldots, w_{pn}}]^{t}\) is weight vector connecting \(p^{th}\) hidden node and input nodes.

\(\beta_p=[\beta_{p1, \beta_{p2}, \ldots, \beta_{pm}]^{t}\) is weight vector connecting \(p^{th}\) hidden node and output nodes.

And \(b_p\) is the threshold of the \(p^{th}\) hidden node. With Activation function \(g(x)\) and \(L\) hidden nodes SLF’s can approximate these \(N\) samples with zero error i.e. \(\sum_{q=1}^{N} \|o_q-t_q\|=0\)

Thus, we can say that there exist \(w_p, b_p\) and \(\beta_p\) such that,

\[
\sum_{p=1}^{L} \beta_p \cdot g(w_p \cdot x_q + b_p) = t_q \quad \text{for} \quad q=1,2,3,\ldots,N
\]

We can also show the above equation as

\[H\beta = T\]

Where \(H(w_1, \ldots, w_L, b_1, \ldots, b_L, x_1, \ldots, x_N)\)

\[
= \begin{bmatrix}
g(w_1 x_1 + b_1) & \cdots & g(w_L x_1 + b_L) \\
\vdots & \ddots & \vdots \\
g(w_1 x_N + b_1) & \cdots & g(w_L x_N + b_L)
\end{bmatrix}_{N \times L}
\]

\[
\beta = \begin{bmatrix}
\beta_1^T \\
\vdots \\
\beta_L^T
\end{bmatrix}_{L \times m} \quad \text{and} \quad T = \begin{bmatrix}
t_1^T \\
\vdots \\
t_N^T
\end{bmatrix}_{N \times m}
\]

When the input weights \((w_p)\) and hidden layer biases \((b_p)\) are determined then output weight \(\beta_p\) is calculated as:

\[\beta = H^+ T\]

Where \(H^+\) is the Moore-Penrose generalized inverse of matrix \(H\).

WEIGHTED EXTREME LEARNING MACHINE

Weighted extreme learning machine could be termed as extreme learning machine with weight matrix and regularization parameter. Regularization parameter is used to represent trade-off between maximizing marginal distance and minimizing misclassification error cost/value and, weight matrix is inversely proportional to the normalized input data.
Training samples are given in the form of \((x_i, t_i)\) where, \(x_i \in \mathbb{R}^n\) and \(t_i\) is either -1 or +1 for \(i=1, \ldots, N\) and \(n\) is the number of features in each training sample. Define an \(N \times N\) diagonal weight matrix for each training sample \(x_i\) where, weight assigned to minority class is always greater than weight assigned to majority class. Input weight \((w_{pj}\) for \(p=1,\ldots,L, j=1,\ldots,n\)) between \(n\) input nodes and \(L\) hidden layer nodes and bias \((b_p\) for \(p=1,\ldots,L\)) at each hidden layer node are randomly generated between 0 and 1. Hidden layer output is \(h_p = w_p x_i + b_p\). Output layer node output is \(y_i = h_b(x_i) \beta_1 + h_{2}(x_i) \beta_2 + \ldots + h_{L}(x_i) \beta_L = h(x_i) \beta\) and output in vector form is \(Y = H \beta\). Target output is \(T = t_1, t_2, \ldots, t_N\). Since it is a binary classifier so there is only one output node. Error vector is \(\xi = Y - T = H \beta - T\). Output weight should be such that the marginal distance is maximum for better generalization performance. Architecture of ELM is shown in fig. 1. So, for maximizing marginal distance and minimizing error vector we can model optimization function as

\[
\text{Minimize: } f = \frac{1}{2} \| \beta \|^2 + \frac{1}{2} CW \sum_{i=1}^{N} \| \xi_i \|^2
\]

Subject to: \(h(x_i) \beta = t_i - \frac{\xi_i}{\xi_t^T}\) for \(i=1,2,\ldots, N\)

Solving this optimization function using Langrange multiplier and Karush-Kuhn-Tucker theorem [2] we get required output weight as

\[
\text{When } N \text{ is small: } \beta = H^T \left( \frac{1}{C} + WHH^T \right)^{-1} WT
\]

\[
\text{When } N \text{ is large: } \beta = \left( \frac{1}{C} + H^T WH \right)^{-1} H^T WT
\]

**Fig.2. Architecture of Weighted ELM**

**WEIGHT DETERMINATION IN WEIGHTED ELM**

In weighted ELM, two schemes for weighing misclassification are given. Minority misclassification weight is given as inverse of total minority samples and majority misclassification weight is given as inverse of total majority samples.

\[
W_{\text{Minority}} = \frac{1}{S(\text{Minority})} \quad \text{and} \quad W_{\text{Majority}} = \frac{1}{S(\text{Majority})}
\]

Where, \(S(\text{minority})\) is the number of samples belongs to minority class and \(S(\text{majority})\) is the number of sample belongs to majority class.

In other scheme, minority misclassification weight is given as inverse of number of minority samples multiplied by 1 and majority misclassification weight is given as inverse of majority samples multiplied by 0.618.

Here, minority misclassification weight is always greater than majority misclassification weight which causes proper positioning of classification boundary and hence determines good generalization performance [9] [10].

**BACTERIAL FORAGING ALGORITHM (BFOA)**

1. Initialize parameters \( p, S, N_s, N_e, N_r, N_{rc}, C(i) = (1, 2, 3, \ldots, S), \theta \)
2. Elimination dispersal-loop: \( l = l+1 \)
3. Reproduction loop: \( k = k+1 \)
4. Chemotaxis loop: \( j = j+1 \)
   a. For \( i = 1, 2, \ldots, S \) take a chemotactic step as follows for bacterium \( I \) as follows
   b. Compute fitness function, \( J(i, j, k, l) \).
   c. Let \( J_{\text{last}} = J(i, j, k, l) \) to save this value since we may find a better cost via run.
   d. Tumble: generate a random vector \( \Delta(i) \) with each element \( \Delta_m(i), m = 1, 2, \ldots, p \), a random number on \([-1, 1]\).
   e. Move: Let \( \theta'(j+1, k, l) = \theta'(j, k, l) + C(i) \Delta(i) \sqrt{\Delta^T(i) \Delta(i)} \) this result in step size \( C(i) \) in the direction of tumble for bacterium \( i \).
   f. Compute \( (i, j+1, k, l) \) and let \( J(i, j+1, k, l) = J(i, j, k, l) + J_{cc}(\theta'(j+1, k, l), P(j+1, k, l)) \) (i.e. add on the cell to cell attractant-repellant profile to simulate the swarming behavior)
   g. Swim
      i. Let \( m = 0 \) (Counter for swim length).
      ii. While \( m < N_s \) (if have not climbed down too long).
         - Let \( m = m+1 \)
         - If \( J(i, j+1, k, l) > J_{\text{last}} \) (if doing better), let \( J_{\text{last}} = J(i, j+1, k, l) \) and let \( \theta'(j+1, k, l) = \theta'(j, k, l) + C(i) \frac{\Delta(i)}{\sqrt{\Delta^T(i) \Delta(i)}} \) and use this \( \theta' \) \( (j+1, k, l) \) to compute the new \( J(i, j+1, k, l) \) as we did in [f]
         - Else let \( m = N_s \). This is the end of the while statement.
   H. Goto the next bacterium \( (i+1) \) if \( i \neq S \) (i.e. go to [b] to process the next bacterium).
5. If \( j < N_r \), go to step 4. In this case continue chemotaxis since the life of bacteria is not over.
6. Reproduction:
   a. For all given \( k \) and \( l \), and for each \( i = 1, 2, \ldots, S \), let \( J_{\text{health}} = \sum_{j=1}^{N_e} J(i, j, k, l) \)
   b. Sort bacteria and chemotactic parameters \( C(i) \) in order of ascending cost \( J_{\text{health}} \) (higher cost means lower health).
5. If \( k < N_r \), go to step 3. In this case, we have not reached the number of specified reproduction steps, so we start the next generation of the chemotactic loop.
8. Elimination-dispersal: For \( i = 1, 2, \ldots, S \) with probability \( P_{\text{ed}} \), eliminate and disperse each bacterium (this keeps the number of bacteria in the population constant). To do this, if a bacterium is eliminated, simply disperse another one to a random location on the optimization domain.

**PROPOSED WORK**

As we have seen that, Weighted ELM is a good approach for classification which overcomes the problem of presence of data with imbalanced class distribution in ELM and also improves the accuracy of ELM but, it is unable to provide optimal solution because, here misclassification cost or weight, which is assigned to binary classes is inversely proportional to the number of samples or we can say that, here, dependency of weight on number of samples exist which restricts search space for finding optimal weights at which good classification accuracy can be achieved.
As we have seen that, no considerable work had been done in this field till date. Therefore, in our proposed weighing scheme, we found weight with the help of MEMETIC Algorithm which is a global search and optimization technique which increases search space. Then these weights are assigned directly to the binary class which eliminates the dependency on number of samples. NGVCK and MWOR kit [3] is taken for generating virus dataset and normal files are taken from windows 7. After applying proposed technique satisfactory results are being achieved. Current work shows better result when compared with WELM_GA and WELM_PSO techniques.

CONCLUSION
This work proposes WELM_BFO for the detection of computer viruses, which improves the performance of WELM and gives optimal misclassification weights. This paper involves the NGVCK and MWOR kits used for malware generation. These kits are broadly used in research due to their property of generating challenging viruses that is not easy to detect. This study will be helpful for those working in the field of computer virology.

ACKNOWLEDGEMENT
I wish to express my special thanks to all who supported me directly or indirectly in this work.

REFERENCES