DETECTION OF COMPUTER VIRUSES USING WELM_FGA_FACO

Ankur Singh Bist

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_FGA_FACO to detect computer viruses. The proposed method efficiently detects static and nature changing viruses.

KEYWORDS: WELM_FGA_FACO, Extreme Learning Machine.

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].

![Figure 1: Assembly code of Virus File](image)

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, \(x_p=[x_{p1},x_{p2},........,x_{pm}]^T\in R^n\) and \(t_p=[t_{p1},t_{p2},........,t_{pn}]\in R^m\)

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

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

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

\(\beta_p=[\beta_{p1},\beta_{p2},........,\beta_{pm}]^T\) 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. \(\sum_{q=1}^{L} ||o_q - t_q||=0\)

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

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

We can also show the above equation as

\[
H\beta = T \quad \text{(1)}
\]

Where \(H(w_{1},........,w_{L},b_{1},........,b_{L},x_{1},........,x_{N})\)

\[
= \begin{bmatrix}
g(w_{1}x_{1} + b_{1}) & \cdots & g(w_{L}x_{1} + b_{L}) \\
\vdots & \ddots & \vdots \\
g(w_{1}x_{N} + b_{1}) & \cdots & g(w_{L}x_{N} + b_{L})
\end{bmatrix}_{N\times L}
\]

\[
\beta = \begin{bmatrix}
\beta_{1}^T \\
\vdots \\
\beta_{L}^T
\end{bmatrix}_{L\times m} \quad \text{and} \quad T = \begin{bmatrix}
t_{1}^T \\
\vdots \\
t_{N}^T
\end{bmatrix}_{N\times m}
\]

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, \(x_i \in R^n\) and \(t_i\) is either -1 or +1 for \(i=1,........,N\) 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 \(p=1,........,L_j=1,........,n)\) between \(n\) input nodes and \(L\) hidden layer nodes and bias \((b_p\) for \(p=1,........,L\)) at each hidden layer node are randomly generated between 0 and 1. Hidden layer output is \(h_p = w_{pj}x_p + b_p\). Output layer node output is \(y_i = h_{1}(x_i)\beta_{1} + h_{2}(x_i)\beta_{2} +........+h_{L}(x_i)\beta_{L} = h(x_i)\beta\) and output in vector form is \(Y = H\beta\). Target output is \(T = t_{1},t_{2},........,t_{N}\).

http://www.ijesrt.com
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

Minimize: \( f = \frac{1}{2} \| \beta \|^2 + \frac{1}{2} CW \sum_{i=1}^{N} \| \xi_i \|^2 \)

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

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

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

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

[Diagram]

**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.

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

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

\[ W_{\text{Minority}} = \frac{1}{\$(\text{Minority})} \quad \text{and} \quad W_{\text{Majority}} = \frac{0.618}{\$(\text{Majority})} \]

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].
GENETIC ALGORITHM

GA(η, χ, μ)

//Initialize generation 0:
K = 0;
P_k = a population of η randomly generated individuals.

//Evaluate P_k:
Compute fitness (i) for each i ∈ P_k;
do

//Create generation k+1

//1. Copy:
Select (1-χ) x η members of P_k and insert into P_{k+1}

//2. CrossOver:
Select (χ x η) members of P_k; pair them up; produce offspring;

//3. Mutate:
Select (μ x η) members of P_{k+1}; invert a randomly-selected bit in each;

//Evaluate P_{k+1}:
Compute fitness (i) for each i ∈ P_k;

//Increment:
K:=k+1;
}

While fitness of individuals in P_k is not high enough.

return the fittest individual from P_k;

η is the number of individuals in the population;
χ is the fraction of population replaced by crossover in each iteration;
μ is the mutation rate.

ANT COLONY OPTIMIZATION ALGORITHM

Algorithm:
1. Create construction graph
2. Initialize pheromone values
3. While not stop-condition do
4. Create all ants solution
5. Perform local search
6. Update pheromone values
7. End while.

The purpose is to unite both methods (GA & ACO) in the best way possible, and the solution that we proposed is to apply fuzzy logic to manage with the uncertainty in both optimization algorithms.

FACO + FGA METHOD

The general approach of the proposed FACO + FGA method can be described as follows:
1. It receives a required function to be optimized.
2. It evaluates the role of both GA and ACO.
3. A main fuzzy system is responsible for receiving values resulting from step 2.
4. The main fuzzy system decides which method to use (GA or ACO).
5. Then, another fuzzy system receives the Error and Derivate of error (DError) as inputs to evaluate if it is necessary to change the parameters in the GA or ACO.
6. There are 3 fuzzy systems. One is for decision making (called main fuzzy), the second one is for changing parameters of the GA (called fuzzyga) and the third fuzzy system is used to change parameters of the ACO (is called fuzzyaco).
7. The main fuzzy system decides in the final step the optimal value for the function introduced in step
8. Repeat the above steps until the termination criterion of the algorithm is met.
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 FACO + FGA method 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.

CONCLUSION
This work proposes WELM_FGA_FACO 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