ISSN:2231-0711

Intrusion Detection System for Malicious Traffic by using PSO-GA Algorithm

K.Pradeep Mohan Kumar

Assistant Professor,Department of Computer Science and Engineering,
Periyar Maniammai University,Thanjavur.

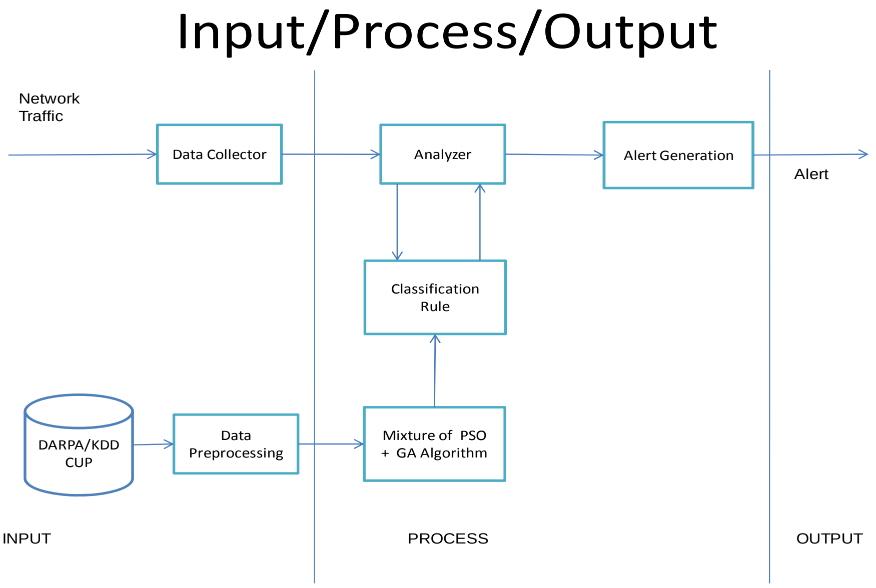
Abstract:In terms of computing, a malicious attack is an attack that can be used to compromise the system state with the intent of acquiring, destroying, modifying or accessing a user's data without any permission. Physical attacks typically mean either the theft of hardware storing personal/confidential information or the destruction of said hardware. Electronic attacks (the focus of this presentation) involve unauthorized access or unauthorized modification of the user's computer. Malicious attacks like Viruses, Worms, Trojan horses, Logic bombs (a.k.a. *Time bombs*), Trapdoors, Phishing/Spoofing can be accessing victim system resources without getting any permission. Earlier detection system like firewall, access control, encryption methods are failed due to self similarity of new malicious attacks. We propose new Intrusion detection system for malicious traffic by using particle swarm optimization techniques combined with genetic algorithm. The main use of this combined algorithm is that it produces good classification rules. By using these rules, IDS detects the intrusion with very low false alarm rate and High detection Accuracy rate.

Keywords: IDS, PSO, GA, Combination of PSO-GA.

INTRODUCTION:

Traditional security policies or firewalls have difficulty in preventing such attacks because of the hidden vulnerabilities contained in software applications. Therefore, intrusion detection system (IDS) is required as an additional wall for protecting systems despite the prevention techniques. Particle swarm optimization (PSO) is the method that receives increasing attention with remarkable results for the design of IDS recently. Unfortunately, the determination of parameters values become an optimization problem in the practicability of PSO. IDS always deal with huge amount of data causing slow training and testing process and low detection rate. So feature selection is one of the key topics in IDS. Thus a new technology namely "A Global optimal search performance of particle swarm optimization (PSO)" is used to select the parameter from the KDD Cup 99 dataset and the resultant parameter model is given to GA. It produces accurate classification rules for IDS. The method is very easy to implement and there are few parameters to adjust.

Block Diagram of PSO-GA based IDS



This paper is organized as follows: Section I introduces Parameters selection of PSO and the feature selection for IDS based on GA is introduced in Section II. Section III briefs about the combination PSO-GA the performance of the proposed model with the data sets.

SECTION I:PSO ALGORITHM:

In a standard PSO algorithm, each dimension of a particle can only be set as real values. So it is hard to be used in discrete optimization problems such as feature selection of network connection records in DARPA data. Data sets with unimportant, noisy or highly correlated features will significantly decrease the classification accuracy rate. By removing these features, the efficiency and classification accuracy rate can be obtained. The basic process of the PSO algorithm is given by:

Step 1: (Initialization) Randomly generate initial particles. For the BPSO algorithm, the complete set of features is represented by a binary string of length N, where a bit in the string is set to ‘1’ if it is to be kept, and set to ‘0’ if it is to be discarded, and N is the original number of features.

Step 2: (Fitness) Measure the fitness of each particle in the population.

Step 3: (Update) Compute the velocity of each particle.
V=m/h; M represent at which time the connection can open.
h represent at which the connection can request.

Step 4: (Construction) For each particle, move to the next position.

Step 5: (Termination) Stop the algorithm if the termination criterion is satisfied; return to Step 2 otherwise.

SECTION: II GENETIC ALGORITHM:

- Input: Data Sets.
- Output: classification Rules.
- GA based on principles of nature selection and evaluation from the data models.
- Process starts with randomly selected population from the data structure.
- GA performs three operations:
- Number of best fit is selected based on user define fitness function.
- Ex: (Source Ip, Dest Ip, Source Port, Dest Port, Protocol, Sender data, receiver data)
- Remaining individuals are paired and thru process of crossover new pairs are created.
- Mutation means randomly changing the bit position in the packet attribute to create new possibilities.

Finally classification rules are created.

GA gets the input data from network traffic (both normal and abnormal data).

Compare with classification rule set.

if { condition } then { act }

If the condition is true then take necessary action.

SECTION: III PSO-GA ALGORITHM:

- Input: Data Sets.
- Output: classification Rules.
- Select the particle from the data set.
- Calculate fitness value.
- If the fitness value better than the best personal fitness in history.
- Set new fitness value as the personal best.
- Select the best fitness value from the set of particles.
- Mutation means randomly changing the bit position in the packet attribute to create new possibilities.

Finally classification rules are created.

GA gets the input data from network traffic (both normal and abnormal data)

Compare with classification rule set.

if { condition } then { act }

If the condition is true then terminate the connection.

EXPERIMENT SETUP AND PERFORMANCE EVALUATION

Data Set and Processing:

The data used here originated from MIT’s Lincoln Labs and is considered a standard benchmark for intrusion detection evaluations. In the experiments, we firstly utilized our feature selection algorithm to select important features, and then built intrusion detection systems using these selected features. The training data set is then separated into attack data sets and normal data sets, which are then subsequently fed into the hybrid PSO - GA algorithms. Through the training process, hybrid PSO- GA models can be built. We then feed the test data set into the PSO-GA models.

Anomaly Detection Result:

The research intends to compare the efficiency of GA and PSO-GA under different circumstances. Detection and identification of attack and non-attack behaviors can be generalized as the following:

True positive (TP): the amount of attack detected when it is actually attack.

True negative (TN): the amount of normal detected when it is actually normal. Thus detection rate is

Detection rate=TP/(TP*TN)*100.

CONCLUSION

In this paper, we proposed a Combined PSO-GA based feature selection algorithm to build IDS. In PSO parameters source Ip, Dest Ip and source pport, Dest Port are selected by PSO and to generate parameter list given to GA to evaluation the performance of IDS. We developed a series of experiments on KDD Cup (1999) intrusion detection dataset to examine the effectiveness of our feature selection and its free parameters in building effective IDS. The experiment results show that our approach is not only able to achieve the process of selecting important features but also to yield high detection rates for IDS. In our future work, we will further improve our feature selection algorithm on search strategy and evaluation criterion to help build efficient and practical intrusion detection.

REFERENCES:

1. ”A General Study of Associations rule mining in Intrusion Detection System” Vikas Markam 1, Lect. Shirish Mohan Dubey 2,Vol 2,Jan 2012.
2. ”MADAM ID FOR INTRUSION DETECTION USING DATA MINING” Amit Kumar Sharma, Feb 2012.
3. ”Multi-agent cooperative intrusion response in mobile adhoc networks” Yi Ping1;2, Zou Futai1, Jan 2007.
4. “INTRUSION DETECTION WITH MOBILE AGENTS” Wayne A. Jansen, Feb 2002.
5. ”RT-MOVICAB-IDS: Addressing real-time intrusion detection”, Álvaro Herrero a, Martí Navarro b,Dec 2010.
6. “A probability agent based Intrusion detection System”, Vaibhav gowadia, May 2005.
7. “CIDS: An agent-based intrusion detection system”, D. Dasgupta*, F. Gonzalez, K. Yallapu, J. Gomez, R. Yarramsettii, Jan 2005.
8. “Intrusion detection throug learning behaviour process”, Balajinath,Raghavan,Nov 2000.
9. ”A new approach to intrusion detection using Artificial Neural Networks andfuzzy clustering”, Gang Wang a,b,*, Jinxing Hao b, Jian Mab, Lihua Huang a, Jan 2010.
10. ”Mutualin formation based features election for intrusion detection systems”, Fatemeh Amiri a,n, MohammadMahdiRezaeiYousefi a, CaroLucas a, Jan 2011.