Student name :salman afridi
Reg ID# 14110
MSCS 2017-2018
SUBJECT:NETWORK MANAGEMENT
MID EXAME 2 ASSIGMENT
DEPARTMENT OF COMPUTER SCIENCE

incorporating Evolutionary Computation for Securing Wireless Network against Cyber threats

Abstract

Due to the rapid growth of Internet services, the demand for network protection and security against complex attacks is increasing. Optimization techniques based on evolutionary algorithms (EA) have been widely used to solve the problem of detecting network anomalies. To solve these limits, in this study, we introduce a new evolutionary hybrid algorithm combining the techniques of Grasshopper Optimization Algorithm (GOA) and Simulated Annealing (SA), called GOSA for IDS which extracts the most remarkable characteristics and eliminates those which are not relevant to the original IDS data sets. Support vector machine (SVM) is used as an adjustment function in the method proposed in this paper to select relevant features that help to accurately classify attacks. It can be seen from the experimental results that the method proposed in this paper surpasses the existing advanced methods, achieving a high detection rate of 99.86%, an accuracy of 99.89%, and a low false alarm rate of 0.009 in the NSL-the detection rate of KDD is as high as 98.85%. The accuracy in UNSW-NB15 is 98.96%, and the false alarm rate is relatively low, 0.084.

1. Introduction

Network security contributes to the security of information systems (such as hardware, software, and related organizations), the data stored on the systems, and the services provided by these systems. Intruders can illegally access this information, and this information can also be used and abused. Sometimes, system operators intentionally cause misuse or damage.
Network security instructions are needed to protect computer systems. The purpose is to require multiple organizations to protect their systems and data (information) from cyber-attacks in addition to enterprises. Despite the contemporary development of computer networks, security applications, and people's understanding of modern defense technologies today, modern devices against the latest cyber attacks still cannot provide comprehensive protection. In order to solve this problem, intrusion detection systems (IDS) are now considered to be effective methods to improve detection capabilities. Compared with traditional network protection technologies (such as firewalls), the intelligence and human-centered IDS that can use interception and information about network intrusions have real value in the network. real world. It can be deployed in a central network backbone or system. Currently, unlike peripheral attackers, the use of smart IDS is seen as an emerging solution for network protection and security. In signature-based IDS, a database of predefined signatures (patterns) is used to compare new activities with known patterns or identified intrusion scenarios, which can be

explicit patterns or data sequences. Perform intrusion detection. It can distinguish attacks by examining network data factors. The network data contains a noisy attribute and persuades other attributes that may reduce the detection accuracy, and entering certain attributes can improve the accuracy of the intrusion detection system. From now on, in order to help the entry of learning methods, the choice of information attributes is crucial for IDS. SF technology is mainly divided into filtering and packaging methods. Generally, filtering methods use metrics of space, information relevance, and consistency to evaluate the selected subset of functions, while encapsulation methods estimate the subset of functions, including classifiers and their functions. As a packaging method, simulated annealing (SA) is a popular heuristic method based on the Metropolis Monte Carlo algorithm, which expands the local search method by using explicit schemes to generate local optimal values. The main contribution of this paper are recorded as:

In order to benefit from the advantages of the GOA and SA algorithms, we propose a new technique for selecting hybrid evolution features, called GOSA. This target is considered to be able to obtain good results related to the performance of the classifier in determining the attack of a given IDS data set based on attributes.

We integrated two wrappers, GOA and SA, which can select the best number of attributes to help identify the type of attack. In addition, GOSA is used to enhance the penalty factor (C) and kernel parameters (σ) of support vector machines.

We are experimenting with standard IDS data sets, such as NSL-KDD and UNSW-NB15 in [20], for simulation and verification. GOSA's performance is evaluated based on several evaluation parameters, such as classification accuracy, execution training and test time, detection rate, and false alarm rate.

2. Related Work

In order to explore the problem of network intrusion detection, in the past few years, researchers have used various types of methods, such as evolution and filtering methods.

In this study, we focus on the SA and GOA hybrid packaging method to detect attacks. In order to deal with linear and nonlinear related data attributes, the author proposes a method based on mutual information to systematically select the best classification attribute.

The effectiveness of the proposed method has been estimated in the event of network intrusion recognition.

Using the attributes selected by the proposed algorithm, an IDS based on square support vector machine (LSSVM-IDS) was fabricated.

Similarly, Javidrad et al. produced a hybrid method consisting of Particle Swarm Optimization (PSO) and Simulated Annealing (SA) methods for optimizing the stacking order of laminated laminates withstand stress. Reach the minimum weight on the airplane and at the moment of bending. The method uses SA as a local search technique to improve the convergence speed of PSO.

GOA has effectively solved many discrete, continuous, multi-objective and single-objective optimization problems for various classical meta-heuristic algorithms (such as DE and PSO) to solve global optimization problems and achieve success.

This is the first time that we use the GOA algorithm for intrusion detection in a hybrid model as a search technique to select the best parameters and reduce the size of the data set.

3. Proposed method

3.1. Binary Grasshopper Optimization Algorithm

In the binary FS problem, by specifying one or more bits of the position vector as a search for space d, the agent of the binary optimization algorithm can only move to the near and far ends of the hypercube. 'Super cube. However, to solve the binary FS problem, this method cannot be used. As mentioned in previous research [28], Mirjalili and Lewis use transfer function, which is an effective method to convert continuum to binary.

3.2. Optimizing SVM parameters with GOSA

GOA is a latest nature-inspired research technique used to find approximate solutions to various real-world engineering problems.

Then, evaluate all aspiring agents by calculating the appropriateness, and regard the best research agent among the current agents as the target. Leader Grasshopper began to attract another person around, and Grasshopper began to move towards Leader Grasshopper.

Similar to other EAs, GOA stays in local optimization when applied to various optimization problems.

Therefore, in order to combine the detection ability of GOA and the local search ability of SA, this paper uses the fusion of GOA and SA (called GOSA) to optimize the parameters σ and C of SVM.

4. Overall Hybrid Approach

In recent years, various evolution methods have been useful in improving the efficiency of IDS systems. In addition, many hybrid technologies should also clarify the shortcomings of each technology. In this part, we are considering using the new hybrid method of GOA and SA to enrich the detection accuracy of IDS.

4.4.1. Data Collection and Pre-processing

Data collection is the first step of intrusion detection. This is the systematic information collection method. Data collection is the first step of intrusion detection. This is the systematic information collection method. Data preprocessing is the longest and most necessary step in the field of data mining. Initially, the data is usually collected from various platforms and has the properties of noisy, inconsistent, incomplete and redundant.

4.4.2. Attack Recognition

In general, it is necessary to create a classifier to distinguish attacks to consider multiple types of problems. In the first part of the experiment in the field used in this article, if the information provided by the record category is used as regular data, the record category is consistent with the regular category, on the contrary, if an attack is envisaged, the opposite is true. At this time, the best parameters are used to train the SVM classifier.

4.4.3. Classification using Hybrid GOSA method

The main reason for the hybridization of GOA and SA is to develop their behavior (group) of social behavior by placing themselves in the best agency position. The main reason for GOA and SA hybridization is to develop their social behavior (group) by placing themselves in the best agent position. The proposed GOSA method responds between GOA and SA, and combines the advantages of GOA's exploration skills and SA's local research capabilities. In this way, the proposed method also improves classification performance by obtaining adjusted support vector machine parameters, avoids stagnation and increases convergence speed, and reduces complexity when seeking to generate a rich set of attributes. Based on abnormal system performance.

5. Experimental Results and discussion

5.1. Experimental Settings

In the MATLAB R2016a environment, a hybrid function selection technology integrating GOA and SA algorithms is implemented. All the experiments observed in this study were conducted on a computer equipped with a Pentium Core i7 processor with 16 GB of RAM running the Windows 8 operating system.

For the proposed GOSA method, a certain number of iterations is fixed at 100, and at the same time, we believe that after 100 iterations, the classifier performance and population of the proposed technique are set at 50.

6. Conclusion

In order to maximize the classification performance and minimize the calculation time of the intrusion detection system, in the existing literature, several evolutionary hybrid algorithms have been introduced.

Different technologies have a unique understanding of solving network security problems. Therefore, integrating more than one algorithm that can reduce the gap between each other is the best way to improve the performance of IDS systems.

Although the hybrid evolution algorithm can bring higher performance, it has almost no disadvantages, such as long calculation time and low diversity.

In order to overcome the existing problems, we introduced a new evolutionary hybrid algorithm for function selection, called GOSA, which combines the characteristics of GOA and SA algorithms. The proposed method not only improves the classification performance, but also reduces the calculation time.

In order to improve the research ability and robustness during the evolution process, we applied the SA mechanism after the GOA stage was completed to obtain the best solution. In addition, GOSA technology is also used to select appropriate SVM parameters, avoiding the problem of overestimating SVM.

The experimental work used two intrusion data sets, such as UNSW-NB15 and NSL-KDD. It is recognized in two cases: first, the classifier has all attributes, and then the classifier has a subset of features obtained from the proposed technique (GOSA). Reasonable results obtained from experimental research indicate that GOSA is better than existing technologies in terms of detection performance, false alarm rate, accuracy, and execution test time. And execution training time.

In UNSW-NB15, it was 98.96%, and the false alarm rate was relatively low at 0.084. Through calculations, this quality can build models more efficiently.