Intrusion Detection System (IDS) Techniques: A Review

Priyanka A. Motekar, Dr. Pradip M. Jawandhiya
M.E (C.S.E.) Scholar, Pankaj Laddhad Institute of Technology and Management Studies, Buldhana-443001, Maharashtra, Sant Gadge Baba Amravati University, Amravati. Email: priyaa.motekar@gmail.com
Principal, Pankaj Laddhad Institute of Technology and Management Studies, Buldhana-443001, Maharashtra. Email: pmjawandhiya@rediffmail.com

Abstract- With the speedy enlargement of net in recent years, laptop systems face multiplied variety of security threats. Despite various technological innovations for data assurance, it's still terribly tough to safeguard laptop systems. Therefore, unwanted intrusions happen once the particular computer code systems area unit running. totally different soft computing based mostly approaches are projected to sight electronic network attacks. This paper presents a varied approaches to network intrusion detection like genetic algorithmic program (GA), associate increased higher cognitive process by rule-list i.e. fuzzy classifier and artificial neural network classifier based mostly approach to network intrusion detection. The project conjointly shows the potency of algorithms in terms of your time for classification. These classification rules area unit accustomed notice networking attacks or intrusions. The projected system is applied on KDDCup99 Dataset to yield additional economical and effective classification rules.

Keywords: Genetic Algorithm (GA), Intrusion Detection System (IDS), artificial neural network (ANN), KDD Cup 1999 Dataset, fuzzy classification, computer and network security.

1. INTRODUCTION

The number of intrusions into laptop systems is growing as a result of new automatic hacking tools area unit showing each day, and these tools in conjunction with numerous system vulnerability data area unit simply obtainable on the online. the matter of intrusion detection has been studied extensively in laptop security and has received plenty of attention in machine learning and data processing. Despite increasing awareness of network security, the prevailing solutions stay incapable of totally protective net applications and laptop networks against the threats from ever-advancing cyber-attack techniques like DoS attack and laptop malware. Developing effective and adaptational security approaches, therefore, has become a lot of vital than ever before. the standard security techniques, because the 1st line of security defense, like user authentication, firewall and encryption, area unit short to completely cowl the complete landscape of network security whereas facing challenges from ever-evolving intrusion skills and techniques thence, another line of security defense is very counseled, like Intrusion Detection System(IDS)

2. LITERATURE SURVEY

Sr. No	Paper Name	Authors	Published Year	Description	Advantages	Disadvantages
1	Three Approaches to Intrusion Detection. Analysis and Enhancements	Pedro A. Diaz-Gomez and Dean F. Hougen	2010	One of the most important responsibilities of every company is to preserve the integrity, confidentiality and availability of its data. Many efforts have been made to accomplish this goal: security policies, firewalls, intrusion	improves the security of information systems	Risk associated with maintenance

				detection systems, anti-virus software, and standards to configure services in operating systems and networks.		
2	Fitness Function for Genetic Algorithm used in Intrusion Detection System	FirasAl absi, Reyadh Naoum	2012	Computer network usage increased rapidly at the last decades, the intruders tried to satisfy their needs by many types of attack depending on the intruder objectives, this encourage the researchers to find more and more solutions to detect those attacks. Intrusion Detection System used to detect the attack. Genetic Algorithm used to support IDS. Fitness Function is helpful in chromosome evaluation which is a Genetic Algorithm part. The problem is to find a suitable Fitness Function for a chromosome evaluation to get a solution for Intrusion Detection.	Efficient results	Not simple to use
3	Review On Classification Based On Artificial Neural Networks	Saravan an Kand S. Sasithra	2014	A neural network model which is the branch of artificial intelligence is generally referred to as artificial neural networks (ANNs). ANN teaches the system to execute task, instead of programming computational system to do definite tasks. To perform such tasks, Artificial Intelligence System (AI) is generated.	The important aspects is solving classificati on problems are discussed	Costly
4	Building an intrusion detection system using a filter-based feature selection algorithm	Moham med A. Ambus aidi, Xiangji an He*,	2014	In this paper, we propose a mutual information based algorithm that analytically selects the optimal feature for	reduce the redundanc y	Unimproved search strategy

		, Priyadarsi Nanda, , and Zhiyuan Tan,		classification. This mutual information based feature selection algorithm can handle linearly and nonlinearly dependent data features. Its effectiveness is evaluated in the cases of network intrusion detection. An Intrusion Detection System (IDS), named Least Square Support Vector Machine based IDS (LSSVM-IDS), is built using the features selected by our proposed feature selection algorithm.		
5	A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection	RenHui Gong, Mohammad Zulkernine, Purang Abolmaesumi	2005	The Internet and local area networks are expanding at an amazing rate in recent years. While we are benefiting from the convenience that the new technology has brought us, computer systems are exposed to increasing security threats that originate externally or internally. Different but complementary technologies have been developed and deployed to protect organizations' computer systems against network attacks, for example, anti-virus software, firewall, message encryption, secured network protocols, password protection, and so on. Despite different protection mechanisms, it is nearly impossible to have a completely secured system.	The technique are cost effective and adaptive.	proposed method worked effectively for the selected datasets

3. EXISTING SYSTEM

Current network traffic data, which are often huge in size, present a major challenge to IDSs. These "big data" slow down the entire detection process and may lead to unsatisfactory classification accuracy due to the computational difficulties in handling such data. Classifying a huge amount of data usually causes many mathematical difficulties which then lead to higher computational complexity. There are approaches such as artificial neural network classifier and fuzzy classifier techniques in the literature.

4. PROPOSED SYSTEM AND ALGORITHM

The key contributions of our proposed system are listed as follows .

This work proposes totally different classification techniques for intrusion detection system (IDS), named genetic formula (GA), Artificial Neural Network (ANN) and symbolic logic classification technique for network intrusion detection. This work that theoretical analysis of mutual info is introduced to guage the dependence between options and output categories. the foremost relevant options ar maintained and accustomed construct classifiers for several categories.

4.1 Genetic Algorithm (GA) based IDS:

Genetic algorithm is optimization technique based on the principle of evolutions and natural selections. The solution to the problem is encoded in chromosome like data structure and GA evolves population using operators like selection, crossover and mutation [4, 5]. Each parameter in a chromosome is called as gene. Genes are selected according to our problem definition [5]. These are encoded on bits, character or numbers. The set of generated chromosome is called a population. The fitness function is used to calculated "goodness" of each chromosome [4]. The algorithm for GA is given below:

4.2 Artificial Neural Network (ANN):

3.1 Problem Statement:

1. Redundant and impertinent options in information have caused a long-term drawback in network traffic classification.
2. These options not slow down the method of classification however conjointly forestall a classifier from creating correct selections, particularly once managing huge information.
3. Low performance.

We conduct complete experiments on well-known IDS dataset named KDD Cup ninety nine

for classification. this can be important in evaluating the performance of IDS since KDD dataset is out-of-date and doesn't contain most novel attack patterns in it. additionally, these datasets area unit ofttimes employed in the literature to guage the performance of IDS.

Different from the detection framework planned system that styles just for binary classification; we have a tendency to style our planned framework to think about multiclass classification issues. this is often to indicate the effectiveness and also the practicability of the planned technique for various approaches shoes.

Artificial neural networks (ANN) consider classification as one of the most dynamic research and application areas. ANN is the branch of Artificial Intelligence (AI). The neural network was trained by back propagation algorithm. The different combinations of functions and its effect while using ANN as aclassifier is studied and the correctness of these functions are analyzed for various kinds of datasets. Theback propagation neural network (BPNN) can be used as a highly successful tool for dataset classification with suitable combination of training, learning and transfer functions. When the maximum likelihood method was compared with back propagation neural network method, the BPNN was more accurate than maximum likelihood method. A high predictive ability with stable and well-functioning BPNN is possible. Multi layer feed-forward neural network algorithm is also used for classification.

4.3 Fuzzy Classifier:

The intrusion detection problem (IDP) is a two-class classification problem: the goal is to classify patterns of the system behavior in two categories (normal and abnormal), using patterns of known attacks, which belongs to the abnormal class, and patterns of normal behavior. With fuzzy rules, the solution to classification problem is based on fuzzy logic concepts.In fuzzy logic, fuzzy sets define the linguisticnotions, and membership functions define the truth-value of such linguistic expressions.

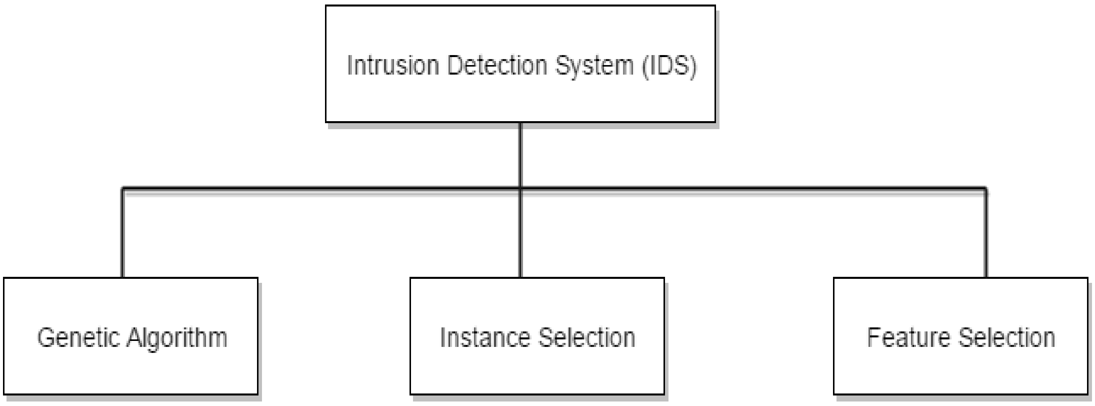

Figure 3.1 Hierarchical Diagram of Technique used

5. CONCLUSION AND FUTURE WORK

In this paper, a system IDS placed at the network egress points to observe malware infections within the network combined network traffic analysis. It projected 3 completely different approaches for network intrusion detection for KDD Cup ninety nine dataset with genetic algorithm(GA), Artificial neural network(ANN) classifier and fuzzy classifier. The experimental results show that this security approach is possible for the property of the system and is nice at sleuthing malware infections attacks. we tend to additionally evaluated the potency of projected algorithms with relevance time needed for classification.

REFERENCES

[1] ChSatyaKeerthi N.V.L., Prasanna P.I., Priscilla B.M., "Instuction Detection system Using Genetic Algorithm",Int. Journal of P2P Network rends and Technology, vol.1.no. 2.pp 1-7, 2011.

[2] Goyal A., Kumar C., "GA-NIDS: A Genetic Algorithm based Network Instruction Detection System", 2008

[3] Mohammad S. H., MukitMd.A.,BikasMd.A. N.," An Implementation of Intrusion Detection System Using Genetic Algorithm", Int.Journal of Network Security and Its Applications, vol.4 no.2.pp 109-119.

[4] Jiang M., Munavar M., Reidemeister T., Ward P.,"Efficient Fault Detection and Diagnosis in Complex Software Systems with Information- Theoretic Monitoring"IEEETrans.On Dependable and Secure Computing.Issue 99, 2011.

[5] ChitturA.,""Model Generation for an Intrusion Detection System Using Genetic Algorithms", 2011.

[6] Lu W., Traore I.," Detecting New Forms of Network Instruction Using Genetic Programming", Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing, Malden, pp. 475-494, 2004.

[7] Pedro A. Diaz-Gomez and Dean F. Hougen "Three Approaches to Intrusion Detection Analysis And Enhancements", National Computer And Information Security Conference Acis2006 .

[8] Li W. "Using Genetic Algorithm for Network Intrusion Detection", Proceedings of the

United States Department of Energy Cyber Security Group, 2004.

[9] Gong R. H., Zulkernine M., Abolmaesumi P.,"A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection", 2005.

[10]Alabsi,F., Naoum,R., "Fitness Function for Genetic Algorithm used in Intrusion Detection System",International Journal of Applied Science And Technology.Vol. 2.no 4, 2012.

[11]Kandeeban,S.S., Rajesh R.S.,"A Mutual Construction For IDS Using GA", Int. Journal of Advance Science And Technology,vol.29, 2011.

[12]Uppalaiah B., Anand K., Narsimha B., warajS., BharatT., "Genetic Algorithm Approach to Intrusion Detection System", IJCST vol.3.1,2012.

[13]Owais S.S.J., Kromer P., Snasel V., "Implementing GP on optimizing Boolean and Extended Boolean Queries in IRs withRespectto Users Profiles", Proc. IEEE lCCES'06 Egypt. pp412-417.2006