ISSN: 2581-3404 (Online)

International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-6, 2019

Efficient Modeling of Intrusion Detection using Evolutionary Approach

Pooja kushwah[1], Prof. Praveen Kataria[2]

[1]M. Tech Scholar, Department of CSE, ASCT, Bhopal (India)

[2]Professor, Department of CSE, ASCT, Bhopal (India)

ABSTRACT

With the high usage of Internet in our day today life, security of network has become the key foundation to all web applications, like online auctions, online retail sales, etc. Detection of Intrusion, attempts to detect the attacks of computer by examining different information records observed in network processes. This can be considered as one of the significant ways to effectively deal with the problems in network security. In this paper we present the comparative experimental study for the intrusion detection and our simulation stats that our proposed method gives better results than the previous techniques.

Keywords: Data mining, Classification, Genetic approach, Intrusion detection.

INTRODUCTION

Intrusion is an unwanted activity in the network and intrusion detection is an important research and development topic with many applications that influencing confidentiality, integrity, availability. In 2014, according to research of Forbes, the most ruthless intrusions include cyber attack stealing personal records of users of eBay, intrusion to Montana Health Department, intrusion effecting P.F. Chang s customers by stealing their credit and debit card numbers, and finally intrusions affecting Evernote and Feedly users. It is clear that intrusion detection is so important for a good security policy.

There are two main approach for security management these approaches are prevention-based and detection-based. In any security plan, if intrusion prevention (encryption, authorization, and authentication) named as the first line of security is passed by attackers, as a second line of defence, intrusion detection comes into prominence. Intrusion detection provides deterrence for intruder and serves an alarm mechanism for a computer system or a network to manage security plan successfully. An intrusion-detection system (IDS) can be defined as software or hardware tools that monitoring network to detect internal or external cyber attacks. An Intrusion Detection System can observe and investigate system and user activities, recognize patterns of known attacks, identify abnormal network activity. General definition of IDS is about intrusions to network but for WSN it can be added that physical damages to sensor devices. Identifying sensor damage is important in order to serve fault tolerance and reliability [13].

An intrusion in the internet can compromise the data security through several internet means. Nowadays, the fast rising networks proliferation, data transfer rate, and an unpredictable Internet usage have added more anomaly problems. Thus researchers need to develop more reliable, effective, and self-monitoring systems, which sort troubles and can, carry out operation devoid of human interaction. By undergoing this kind of attempts, catastrophic failures of susceptible systems can be reduced. Detection stability and detection precision are two key indicators used to evaluate IDS (Intrusion Detection System). Many of the IDS research studies have been done in order to improve the detection stability and detection precision. In the beginning stage, the research work focus lies in using statistical approaches and rule-based expert systems. But, the results of statistical approaches and rule-based expert systems were not accurate, when encountering larger datasets. In order to overcome the abovementioned problem, many data mining techniques were developed [8]. An Intrusion Detection System is designed to detect an intrusion while it is in progress, or after it has occurred. The major functions performed by IDS are monitoring users and systems activity, auditing system configurations, recognizing known attacks, identifying abnormal activities, managing audit data, highlighting normal activities, correcting system configurations and storing information about intruders [4].

The Intrusion Detection Systems are classified as network intrusion detection systems and host-based intrusion detection systems. It is also possible to categorize IDS by its detection approach: the most well-known variants are signature-based detection and anomaly-based detection [12]. Different categories of IDS include Host-based IDS (HIDS), Network-based IDS (NIDS), (HIDS), and Wireless IDS [1]. There is Hybrid IDS which combines various IDS categories. Host-based IDS monitors the activities of a single host and detects if any malicious activity happen. HIDS mainly monitors the process activities and ensure security policies of system files, system logs and registry keys. Anomaly detection techniques are useful in intrusion detection systems since an intrusion activity is different from the normal activity of the system. Host based intrusion detection systems run on individual systems which includes the techniques for collecting and analyzing the information on a particular system [14].

The rest of this paper is organized as follows in the first section we describe an introduction of about intrusion detection and their types and techniques. In section II we discuss about the host based intrusion detection techniques, in section III we discuss about the experimental work. In section IV we discuss about the proposed algorithm and their procedure, and finally in section V we conclude and discuss the future scope.

II HOST BASED IDS

The objective of the HIDS is the controlling state and dynamic behaviour of the computer system. This detection system checks all the activities of inspected packets on a network. HIDS recognize what resources are being utilized and which program gets to those resources. If in the network any alternations or adjustment happens, system administer receive some network alerts. HIDS is progressively becoming essential to ensure the host computer frameworks and its network activities. HIDS with host based information is incorporated into the computer frameworks to identify the intruder abnormal activities, noxious Behaviour, application abnormalities and preserve the Information Systems from intruders and report the occasions to the HIDS System Administrator.

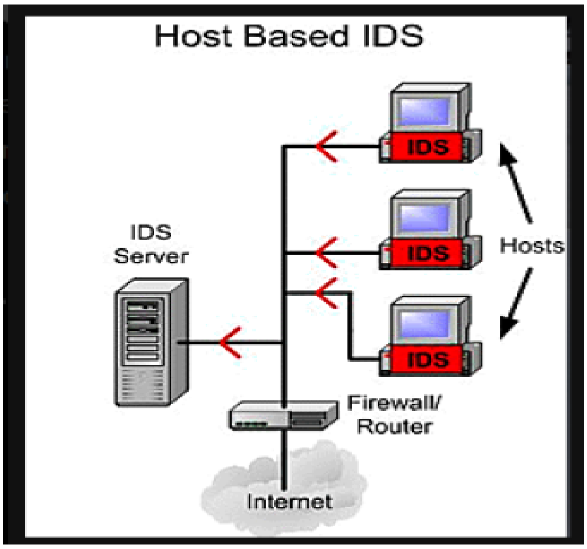


Fig 1: Architecture of Host based IDS.

III EXPERIMENTAL WORK

In the presents scenario it is very challenging to maintain and used the classification of data and detection of network intrusion detection due to large and unknown number of attacker. Day to day come into new format and dynamic nature based attack pattern for the system i.e. host based and network based. To enhance the performance of intrusion detection system we used various types of techniques on the basis of their functionality and their behavior such as data mining, machine learning, evolutionary approach and swarm intelligence etc., where we adopted such types of techniques on the basis of requirement for the system and the types of attacker.

In this paper we proposed a new model for the intrusion detection in a host based and network based, here we used the evolutionary approach such as genetic algorithm for the proposed methods and compare with the existing technique i.e. classification method. Here we used the matlab simulator for the detection of intrusion and the input dataset is kddcup99.

Genetic algorithm uses as an evolutionary approach for the detection of dataset either normal or abnormal, this methods works on the basis of fitness function, this function define the survival of fitness for the particular dataset; initially we select the some sample form the population dataset and then apply the crossover and mutation function, after applying the both function we compare the particular obtain value with the fitness value if condition is satisfied we used this value as a result otherwise repeat the whole process again.

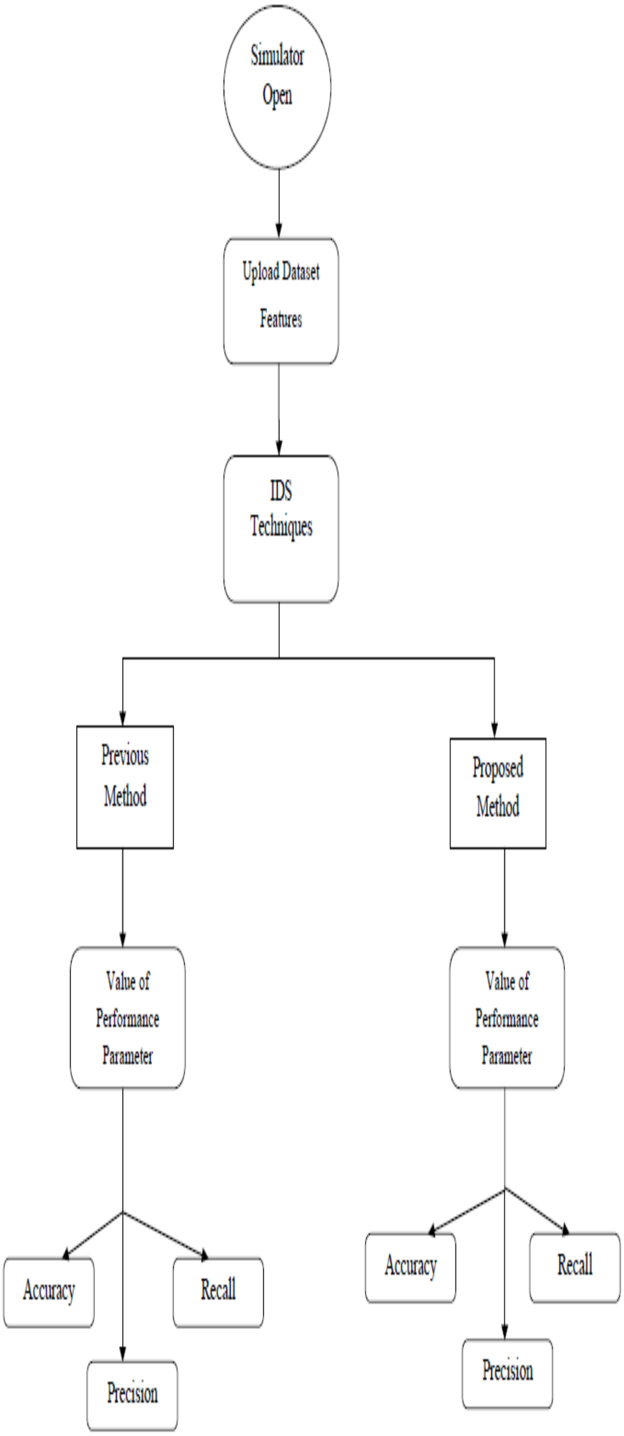


Fig 2: Flow graph for the intrusion detection system.

IV PROPOSED ALGORITHM

1. Generate random population of *n* chromosomes (suitable solutions for the problem)
2. Evaluate the fitness *f(x)* of each chromosome *x* in the population
3. Create a new population by repeating following steps until the new population is complete
a. Select two parent chromosomes from a population according to their fitness (the better fitness, the bigger chance to be selected)
b. With a crossover probability cross over the parents to form new offspring (children). If no crossover was performed, offspring is the exact copy of parents.
c. With a mutation probability mutate new offspring at each locus (position in chromosome).
d. Place new offspring in the new population
4. Use new generated population for a further run of the algorithm
5. If the end condition is satisfied, **stop**, and return the best solution in current population
6. Go to step **2.**

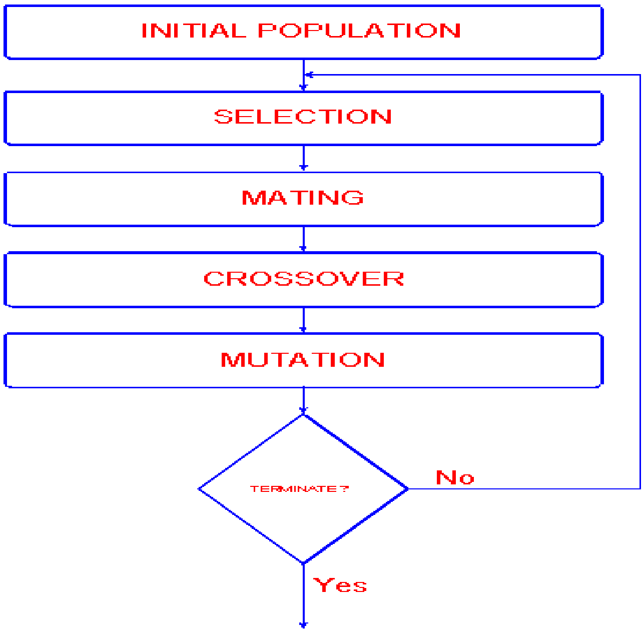
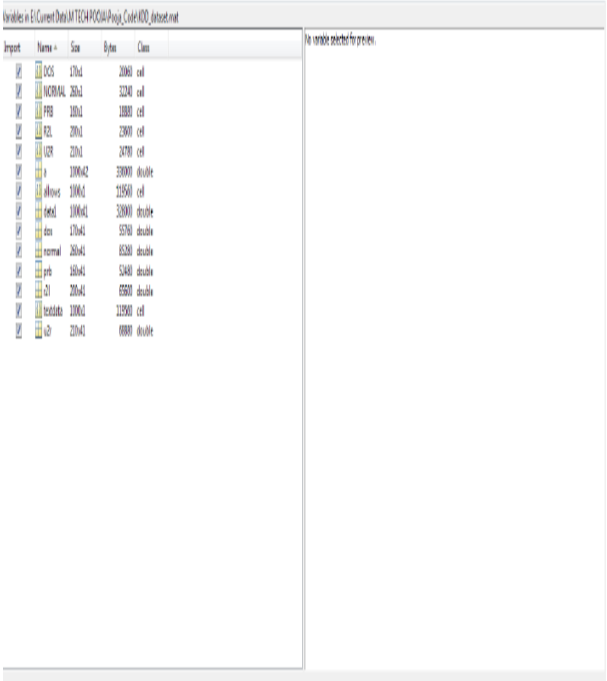


Fig 3: Flow graph for the genetic algorithm procedure.


Variables in E:\Current Data\M TECH POOJA\Pooja_Code\KDD_dataset.mat

Import	Name ▲	Size	Bytes	Class
☑	DOS	170x1	20060	cell
☑	NORMAL	260x1	32240	cell
☑	PRB	160x1	18880	cell
☑	R2L	200x1	23600	cell
☑	U2R	210x1	24780	cell
☑	a	1000x42	336000	double
☑	allrows	1000x1	119560	cell
☑	data1	1000x41	328000	double
☑	dos	170x41	55760	double
☑	normal	260x41	85280	double
☑	prb	160x41	52480	double
☑	r2l	200x41	65600	double
☑	testdata	1000x1	119560	cell
☑	u2r	210x41	68880	double

No variable selected for preview.

Fig 4: Upload the Dataset.

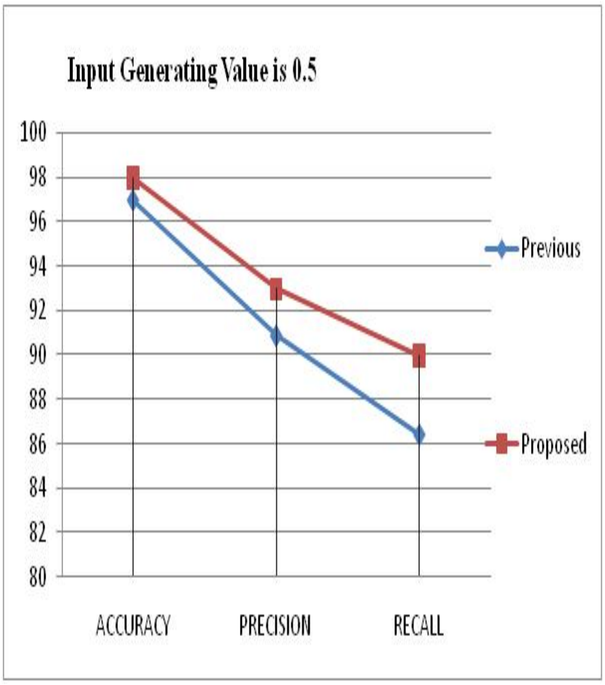


Fig 5: Comparative experimental work for the input value is 0.5.

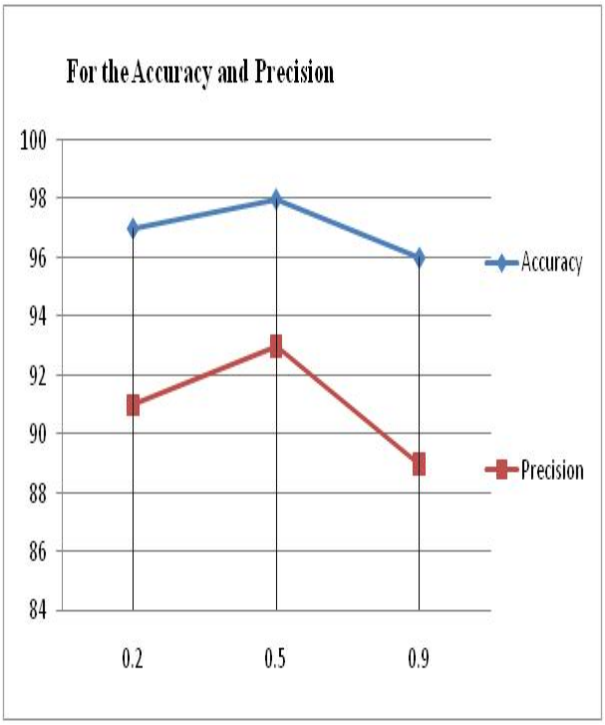


Fig 6: Comparative experimental work for the accuracy and precision.

V CONCLUSION AND FUTURE SCOPE

Ensuring security has always been a challenging problem for both customized network solutions and information systems. Intrusion Detection System (IDS) is playing a very important role to ensure security both in network solutions and information systems. In this paper we present the comparative performance evaluation for the intrusion detection using the classification and genetic method, the proposed method gives better results in terms of accuracy, precision and recall. In future work we can also work on the feature reduction or selective features work with using the KDD dataset.

REFERENCES:-

[1] Pierre-Francois Marteau, "Sequence Covering for Efficient Host-Based Intrusion Detection", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 14, NO. 4, APRIL 2019, pp 944-1006.

[2] Ashima Chawla, Brian Lee, Sheila Fallon, and Paul Jacob, "Host Based Intrusion Detection System with Combined CNN/RNN Model", Springer Nature Switzerland August 2019, pp 149-158.

[3] Md. Zahangir Alom, Venkata Ramesh Bontupalli, and Tarek M. Taha, "Intrusion Detection using Deep Belief Networks", IEEE 2015, pp 339-344.

[4] Hebatallah Mostafa Anwer, Mohamed, Farouk, Ayman Abdel-Hamid, "A Framework for Efficient Network Anomaly Intrusion Detection with Features Selection", IEEE 2018, pp 157-162.

[5] Nutan Farah Haq, Musharrat Rafni, Abdur Rahman Onik, "Application of Machine Learning Approaches in Intrusion Detection System: A Survey", (IJARAI) International Journal of Advanced Research in Artificial Intelligence, Vol. 4, No.3, 2015, pp 9-18.

[6] Rana Aamir Raza Ashfaq , Xi-Zhao Wang , Joshua Zhexue Huang , Haider Abbas , Yu-Lin He , "Fuzziness based semi-supervised learning approach for intrusion detection system", Elsevier 2016, pp 484-497.

[7] Anna L. Buczak and Erhan Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 2, SECOND QUARTER 2016, pp 1153-1176.

[8] JABEZ J, Dr.B.MUTHUKUMAR, "Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach", Procedia Computer Science 48 2015, pp 338 – 346.

[9] M Firoj kabir,Sven Hartman, "Cyber Security:Challenges An efficient Intrusion Detection System Design",IEEE 2018, pp 19-24.

[10] Poonam Sinai Kenkre, Anusha Pai, and Louella Colaco, “Real Time Intrusion Detection and Prevention System”, Springer International Publishing Switzerland 2015, pp 405-411.

[11] Pierre-Francois Marteau, “Sequence Covering for Efficient Host-Based Intrusion Detection”, JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. X, FEBRUARY 2018, pp 1-14.

[12] G. Yedukondalu, J. Anand Chandulal and M. Srinivasa Rao, “Host-Based Intrusion Detection System Using File Signature Technique”, Springer Nature Singapore Pte Ltd. 2017, pp 225-232.

[13] Okan CAN, Ozgur Koray SAHINGOZ, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks”,IEEE 2015, pp 1-6.

[14] Shijoe Jose, D.Malathi, Bharath Reddy, Dorathi Jayaseeli, “A Survey on Anomaly Based Host Intrusion Detection System”, NCMTA 2018, pp 1-11.

[15] MING LIU, ZHI XUE, XIANGHUA XU, CHANGMIN ZHONG, JINJUN CHEN, “Host-Based Intrusion Detection System with System Calls: Review and Future Trends”, ACM Computing Surveys, Vol. 5, November 2018, pp 1-36.

[16] ALEKSANDAR MILENKOSKI, MARCO VIEIRA, SAMUEL KOUNEV, “Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices”, ACM Computing Surveys, Vol. 48, September 2015, pp1-41.

[17] Rafath Samrin, D Vasumathi, “Review on Anomaly based Network Intrusion Detection System”, ICEECCOT 2017, pp141-147.

[18] Nasrin Sultana,Naveen Chilamkurti,Wei Peng ,Rabei Alhadad, “Survey on SDN based network intrusion detection system using machine learning approaches”, Springer Nature 2018, pp 1-9.