IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

A Perspective Study on Network Intrusion Detection System Using Various Approaches

K.Soundarraj[1*], M.Ravichandran[2]

[1,2]Department of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore, India

[*]*Corresponding Author: soundarraj28@gmail.com, Tel.: 9789135332*

Available online at: www.ijcseonline.org

Accepted: 16/Dec/2018, Published: 31/Jan/2019

***Abstract*:-** With the increasing demand on automation and computers, one of the chief issues in the present decade has been to build a secure network, to prevent against malicious activities on the network. The process which monitors and analyzes the communication of network and detects intrusion and anomalies is termed as Intrusion Detection System (IDS). By handling such huge voluminous network traffic-based IDS also creates new issues. To overcome this, many statistics, machine learning and artificial intelligence-based approaches were started evolving. This paper focuses on the importance of such techniques in the field of intrusion detection by performing detailed survey. It presents a general overview of IDS, types of IDs and various methods used for classification. It also describes the several methods and the importance of IDSs in information security.

Keywords:-Intrusion Detection System, Machine Learning, Artificial Intelligence, Statistics, Data mining and Neural Networks

I. INTRODUCTION

In current information era, majority of the modern business mainly rely on computers and networks. With advancement in the field of internet, its usage has been exponentially utilized many of the commercial activities. At the same time security threats are also a very challenging issue which also grows in a rapid manner thus processing and preserving confidential information's through network is a very significant issue for researchers. An Intrusion Detection System (IDS) [14] is an application or device that monitors in the network and/or system activities for malicious activities or policy violations and produces reports to the Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion Detection and Prevention Systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop, and report to security administrators. In addition to that, organizations are use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs become a necessary addition to the security infrastructure of nearly every organization.

There are two main types of IDS's: network-based and host-based IDS. In a network-based intrusion-detection system (NIDS), the sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. The sensor captures all the network traffic and analyzes the content of individual packets for malicious traffic. In a host-based system, the sensor usually consists of a software agent, which monitors all activities of the host on which it is installed, including file system, logs and the kernel.

In a misuse detection approach [12], abnormal system behavior is defined first, and then all other behaviors are defined as normal. It stands against the anomaly detection approach which utilizes the reverse: defining normal system behavior first and defining all other behavior as abnormal. With misuse detection, anything not known is normal.In data mining, anomaly detection is referred to the identification of items or events that do not conform to an expected pattern or to other items present in a dataset.

II. LITERATURE SURVEY

Kumar and Yadav [1] use ANN neural networks method using the KDD cup '99 dataset and shows high anomaly detection by using a gradient descent with momentum back propagation algorithm to train the system in detection. Their method was as efficient in detection and classification of attacks as current methods implemented but only used random patterns of data were used for training Aljurayban and Emam [2] propose the use of a Layered Intrusion Detection Framework (LIDF) for efficient protection of a Cloud networking environment using an Artificial Neural

Network (ANN) to create a data mined knowledge base for detection.

Lobo and Russo [3] investigates the occurrence of Multi-path routed attacks where an attack is fragmented and sent over multiple routes to attempt to fool an IDS system. This is made possible due to multi path TCP (MPTCP) which allows transmissions to route over multiple paths between a source and target.

Anazida Zainal et al. [4] in paper has discussed the Efficiency is one of the major issues in intrusion detection. Inefficiency is often attributed to high overhead and this is caused by several reasons. The purpose of the paper is to address the issue of continuous detection by introducing traffic monitoring mechanism. In traffic monitoring, a new recognition paradigm is proposed in which it minimizes unnecessary recognition. Therefore, the purpose of traffic monitoring is two-folds; to reduce amount of data to be recognized and to avoid unnecessary recognition. For this Adaptive Neural Fuzzy Inference System and Linear Genetic Programming to form ensemble classifiers that shows a small improvement using the ensemble approach for DoS and R2L classes (attacks).

G. Zhai et al. [5] in paper has discussed that ID3 algorithm was a classic classification of data mining. It always selected the attribute with many values. The attribute with many values wasn't the correct one, it would create fault alarm and omission alarm. To this fault, an improved decision tree algorithm was proposed. The decision tree was created after the data collected classified correctly. With the help of using Decision tree algorithm it shows the maximum attacks and also increases the alert level after modified the decision tree.

Jorge Blasco et al. [6] in paper has studied that one of the central areas in network intrusion detection is how to build effective systems that are able to distinguish normal from intrusive traffic. To avoid the blind use of GP, it provides the search by means of a fitness function based on recent advances on IDS evaluation. For the experimental work use of a well-known dataset (i.e. KDD- 99) that has become a standard to compare research although its drawbacks. Results clearly show that an intelligent use of GP provides better accuracy and also compare the Hit rate and False Rate to detect the number of attacks.

Ahmed Youssef et al. [7] in paper has studied that Intrusion detection has become a critical component of network administration due to the vast number of attacks persistently threaten our computers. Traditional intrusion detection systems are limited and do not provide a complete solution for the problem. However, in many cases, they fail to detect malicious behaviors (false negative) or They fire alarms when nothing wrong in the network (false positive). For this combination of Data Mining Techniques and Network behavior analysis were applied and overcome the limitations of traditional Intrusion Detection System.

Mohd. Junedul Haque et al. [8] in paper has said that the Intrusion Detection system is an active and driving secure technology to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a network. The main part of Intrusion Detection Systems (IDSs) is to produce huge volumes of alarms. The interesting alarms are always mixed with unwanted, non interesting and duplicate alarms. For this Data mining algorithm, K means clustering, Distributed IDS are applied to improve the detection rate and decrease the false alarm rate.

S. Devaraju et al. [9] in paper has discussed about the security purpose in information system. To deal with the problems of networks different classifiers are used to detect the different kinds of attacks. In this, the performance of intrusion detection with various neural network classifiers is compared. In this proposed research there are five types of classifiers used. They are Feed Forward Neural Network (FFNN), Elman Neural Network (ENN), Generalized Regression Neural Network (GRNN), Probabilistic Neural Network (PNN) and Radial Basis Neural Network (RBNN). Finally, it is clear that Probabilistic Neural Network has better accuracy than rest of other neural networks.

S.A.Joshi et al. [10] in paper has presented that with the tremendous growth in information technology, network security is one of the challenging issue and so as Intrusion Detection system (IDS). The traditional IDS are unable to manage various newly arising attacks. To overcome this type of problem Data Mining techniques, Feature Selection, Multiboosting were applied. With data mining, it is easy to identify valid, useful and understandable pattern in large volume of data. Features are selected using binary classifiers for more accuracy in each type of attack. Multiboosting is used to reduce both the variance and bias. Thus, the efficiency and accuracy of Intrusion Detection system are increased and security of network so is also enhanced.

In this paper [11] K-means algorithm is used for detecting the normal or Denial of Service (DOS) attack category. The KDD Cup 1999data set is used for evaluate the proposed model. A K-means clustering algorithm is a data mining technique based on this, the network data can be categorized into either normal or abnormal.

In paper [13] presented a neural network-based intrusion detection method for the internet-based attacks on a computer network. Intrusion detection systems (IDS) have been created to predict and thwart current and future attacks. Neural networks are used to identify and predict unusual activities in the system.

Mostaque Md. Et.al. [15] proposes a combinatorial method of applying genetic algorithm and fuzzy logic for the detection of intrusions. The genetic algorithm is applied for generating intrusive rules from the network traffic and then Fuzzy Logic is applied for the optimization of classified values.

Prabhdeep Kaur et. al. [16] uses the fuzzy logics for the network intrusion detection. The Fuzzy Logic are used for the generation of if-then rules for the correctly identification of normal and abnormal attacks. Since intrusion detection can be classified as misuse and anomaly detection approach which can be classified as known and un-known attacks.

III. PROBLEM DEFINITION

The main motivation of this study is to analyze the existing issues in the field of intrusion detection system and defining the goal to overwhelm the issues in the future by considering this major the below mentioned problems

- The first major issue is to improve the quality of the dataset which is under consideration for handling IDS in network. The irrelevant and redundancy prevail in the raw dataset has to be identified to increase the efficiency of the intrusion detection model
- The second toughest dispute in IDS is that the dataset has collected generally consist of imprecise knowledge and uncertainty will greatly affect the performance of the detection model so knowledge in uncertainty handling based model has to be developed
- The third issue is that while developing the models based on the classification they highly produce more number of rules depending on the volume of dataset involved in IDS process. The rule optimization and fine tuning them is an credential need and such supporting optimal model needs to be developed.
- The fourth is introducing, improvised unsupervised clustering techniques in Intrusion detection when the instances are unlabeled. The pattern recognition has to be done with appropriate decision-making approaches.

IV. CONCLUSION

This paper focused on the IDS concept utilized in the various fields but this IDS concept plays very vital role in the Network Environments. This paper studies many existing works in the field of intrusion detection system by using machine learning, data mining and artificial intelligence system have been proposed and are in use currently. Still there are many problems by handling the vagueness information, voluminous dataset processing, enriching quality of the dataset used for intrusion detection. This paper gives importance of the challenges in detection of intrusion in the network. Furtherly the work aims to develop several models to overwhelm the issues signified in this study.

V. REFERENCES

[1] Kumar, S, Yadav A, Increasing Performance Of Intrusion Detection System Using Neural Network, Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on, p546-550, May 2014.

[2] Aljurayban, N.S.; Emam, A. Framework for Cloud Intrusion Detection System Service, Web Applications and Networking (WSWAN), 2nd World Symposium, pp 1-5, 2015

[3] Jiefei Ma; Le, F.; Lobo, J.; Russo, A, Detecting Distributed Signature-based Intrusion: The Case of Multi-Path Routing Attacks. Computer Communications (INFOCOMIEEE Conference on, p558-566, 2015

[4] Anazida Zainal, Mohd Aizaini Maarof and Siti Mariyam Shamsuddin "Data Reduction and Ensemble Classifiers in Intrusion Detection" in 2008 IEEE.

[5] Guangqun Zhai, Chunyan Liu "Research and Improvement on ID3 Algorithm in Intrusion Detection System" in 2010 IEEE.

[6] Jorge Blasco, Agustin Orfila, Arturo Ribagorda "Improving Network Intrusion Detection by Means of Domain-Aware Genetic Programming" DOI 10.1109/ARES.2010.53 in IEEE 2010.

[7] Ahmed Youssef and Ahmed Emam "Network Intrusion Detection using Data Mining and NetworkBehavior Analysis" International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Dec 2011.

[8] Mohd. Junedul Haque, Khalid.W. Magld, Nisar Hundewale "An Intelligent Approach for Intrusion Detection Based on Data Mining Techniques" in 2012 IEEE.

[9] S. Devaraju, S .Ramakrishnan "Detection of Accuracy for Intrusion Detection System using Neural Network Classifier" International Journal of Emerging Technology and Advanced Engineering(ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013).

[10] S.A.Joshi, Varsha S.Pimprale "Network Intrusion Detection System (NIDS) based on Data Mining" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 1, January 2013.

[11] G. Mageswary1 , Dr. M. Karthikeyan2 Intrusion Detection Using Data Mining Techniques International Journal of Engineering Science Invention (IJESI) ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726 www.ijesi.org || PP. 20-25

[12] Helman, Paul, Liepins, Gunar, and Richards, Wynette, "Foundations of Intrusion Detection," The IEEE Computer Security Foundations Workshop V, 1992

[13] J. Shun and H. A. Malki, "Network Intrusion Detection System Using Neural Networks," *2008 Fourth International Conference on Natural Computation*, Jinan, 2008, pp. 242-246.

[14] Butun, Ismail; Morgera, Salvatore D.; Sankar, Ravi (2014). "A Survey of Intrusion Detection Systems in Wireless Sensor Networks". IEEE Communications Surveys & Tutorials

[15] Mostaque Md. Morshedur Hassan," Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic", IJIRC2013.

[16] Prabhdeep Kaur, Sheveta Vashisht "Mingle Intrusion Detection System Using Fuzzy Logic", IJEAT 2013.

Authors Profile

Mr.K.Soundarraj pursed Bachelor of Science from Bharathiar University, Coimbatore in 2007 and Master of Science from Bharathiar University in year 2009. He is currently pursuing Ph.D. and working as Assistant Professor in Department of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Bharathiar University, Coimbatore since 2010. He has presented more than 06 research articles in reputed conferences. His main research work focuses on Genetic Algorithms, Network Security, Big Data Analytics, Data Mining. He has 9 years of teaching experience and 4 years of Research Experience.

Dr.M.Ravichandran Bachelor of Science from Madras University and Master of Science from Bharathiar University in year 1986. He is currently working as Associate Professor in Department of Computer Science, Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Bharathiar University , since 1989. He has published more than 8 research papers in reputed international it's also available online. His main research work focuses on Software Engineering,Data Mining and Big Data Analytics. He has 29 years of teaching experience and 18 years of Research Experience.

