A Survey Based On Intrusion Detection System

Divya Lakshmi K
Department of Information Technology
APJ Abdul Kalam Technological University
Government Engineering College , Barton Hill
divyakozhakkottil@gmail.com

Divya Prasad K H
Assistant Professor
Department of Information Technology
Government Engineering College , Barton Hill
divyaprasadkh@gmail.com

***Abstract* - Anomaly detection is done inorder to identify the network and computer misuse and intrusions and classify them as either normal or anomalous. Artificial immune system, a novel computational intelligence technique which is inspired by immunology is one of the methods used for anomaly detection and it has many wide applications in other areas too. In this paper, presented a survey based on anomaly detection and prevention system. Also have discussed different techniques used for anomaly detection and comparison between those papers and their advantages over other related papers.**

Index Terms-Anomaly detection, artificial immune system, intrusion, immunology.

1. INTRODUCTION

An intrusion detection system (IDS) is used for monitoring the users' activity and network traffic inorder to distinguish between hostile and non-hostile traffic. For intrusion detection, most of current networks implement anomaly detection or misuse detection techniques. The anomaly-based detection system, which is an intrusion detection system is used for detecting both computer and network misuse and intrusions by monitoring the activities of the system and classify them as either normal or anomalous. By detecting the anomalies in the behavior of the processes and systems is significant while predicting their behavior. In data mining, anomaly detection which is also known as outlier detection is the process of identifying observations, items or events that do not conform to an expected pattern or other items in a dataset. For IDS, anomaly detection is accomplished with statistics and thresholds, but they can also be done with soft computing and inductive learning. Anomaly detection ha a wide variety of application domains, such as fraud detection, intrusion detection, fault detection, event detection in sensor networks, system health monitoring and detection of eco-system disturbances. Anomaly detection is often used in preprocessing inorder to remove anomalous data from the dataset. In case of supervised learning, removal of anomalous data from the dataset results in a significant increase in accuracy.

The biological immune system is an adaptive system that defends the body from foreign pathogens. It is possible to categorize all cells within the body as self cells or non-self cells. This is done with the help of a distributed task force which has the intelligence to take actions from a local and a global perspective using its network of chemical messengers for communication. A novel computational intelligence technique, inspired by immunology, has emerged, called Artificial Immune Systems. Artificial Immune Systems (AIS) are adaptive systems that are inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving. Focusing on the AIS state-of-the-art techniques for classification, most of them were based on the self-non-self discrimination. The self-non-self discrimination is an immunological concept which states that the biological immune system is characterized by its pattern recognition capacity that may be used for distinguishing between foreign cells entering the body, which is known as the non-self elements and the body's own cells, known as the self-elements.

The organization of the remaining part of this paper is as follows: a theoretical presentation of the background of related work in anomaly detection and prevention system was presented in section 2. Comparison between related works was discussed in section 3. Section 4 finally discuss about the conclusion of this survey.

2. RELATED WORKS

The related papers that describes about different techniques that are used for anomaly detection and prevention systems are described below:

In (1), Wael Khreich ,Babak Khosravifar ,Abdelwahab Hamou-Lhadj , Chamseddine Talhi proposed an anomaly detection system which is based on variable N-gram features and one class support vector machine. The objective of the proposed system was to reduce false rate. The system combines the frequency with the temporal information from system call traces and one class support vector machine detector. The proposed feature extraction approach begins with segmentation of system call traces into multiple N-grams of variable length and they were mapped to fixed-size sparse feature vectors. These were used to train the one class support vector machine detectors. Higher level of detection accuracy is obtained by combining proposed one class support vector machine detector with the Gaussian kernel trained on feature vectors.

In (2), StratisKanarachos, Stavros-Richard G.Christopoulos , Alexander Chroneos ,Michael E. Fitzpatrick introduced a new signal processing algorithm for detecting anomalies in time series data through deep learning algorithm which combines wavelets, neural networks and Hilbert transform. This algorithm is inspired by deep learning paradigm. The algorithm learns the normal behavior of the system and for assessing the statistical significance there is no need for the existence of anomalous data. Using probabilistic receiver operating characteristics the instantaneous frequency and amplitude of the residual signal are analysed hierarchically for detecting the anomalies. This method could be used to predict earthquake activity because this method is able to detect anomalies in the seismic electric signal. The proposed method is used only for reconstructing the normal behavior of the system. Use of neural networks facilitates online training and facilitates learning short and long-term pattern interdependencies. Without any manual tuning effort the proposed method is successfully applied. The main contributions include proposition of unique deep neural network structure for reconstructing the normal behaviour of the system and feature selection of the anomaly detector. The algorithm is fast, performs robustly and is transferrable.

In (3), Syed Rizvi0F, Gabriel Labrador, Matt Guyan, Jeremy Savan presents a hybrid solution in which signature and anomaly based systems are incorporated to detect and prevent more malicious attacks than usual . This is done by intensifying what is catalogued to include common anomalies to baseline that is used by the signature system. This is an improvement in the framework for the current host IDPS/network that uses signature and anomaly based methodologies .This is done by implementing a hybrid VMM based Honeypot into a theorized self-healing hybrid IDPS and this is for improving the efficiency and accuracy. The internet traffic that is coming from router are passed through firewall and if intrusion is found out then they are immediately blocked. In the proposed solution there are two routes through which the traffic is directed by VM hybrid honeypot, low interaction honeypot or high interaction honeypot. If the traffic is already known then the traffic will passed to high honeypot section and if the traffic is unknown, then traffic is directed towards low honeypot section. The proposed system is efficient, reliable and reduces resource consumption.

In (4), Lalitha K V and Josna V R presented a Gaussian mixture model for verifying traffic. In that the traffic is captured and this is given to the model for verification. The normal behaviour of the network traffic is modelled using Gaussian Mixture Model (GMM).The traffic characteristics are aggregated for a period of time and is given to the model to check the validity of the traffic. The anomaly is detected when the traffic disobeys the model. If the traffic obeys the model, the traffic is normal. It is seen that the unique characteristics are obeyed by various types of network. The parameters used by GMM for modelling traffic are packet train length and packet train size. Sensor network creation and its configuration is the initial step. Cluster formation takes place when sufficient numbers of sensor nodes are added into the network. The traffic which is generated is given as input to the traffic verification system once the communication begins. After this the traffic which are anomalous are identified. The proposed system has better performance in terms of delay, throughput and packet delivery ratio. The proposed system is effectively used in sensor networks and efficient in detecting the anomalies in the traffic.

In (5), Jabez J And Dr.B.Muthukumar proposed a new approach called outlier detection for detecting anomalies. In the outlier detection approach the anomaly datasets is measured by the Neighbourhood Outlier Factor (NOF).In that, inorder to improve the performance of intrusion detection system (IDS)trained model consists of big datasets with distributed storage environment. And develop an IDS based anomaly detection model which would be precise, not easily cheated by small variations in patterns, low in false alarms, adaptive and be of real time. The intrusion packets that received from the internet are collected by SNORT. At the initial, the features are extracted from data packets and then it is forwarded to the proposed IDS. The distance between the extracted features and trained model is computed by the proposed IDS. When the outlier value is greater than the specified threshold then the false alarm is generated which implies the presence of anomaly. And if the outlier value is less than the threshold then it implies there is no anomaly. The advantages of the proposed system are less execution time and less trained datasets.

In [6], Praneet Saurabh, Bhupendra Verma introduced “An Efficient Proactive Artificial Immune System based Anomaly Detection and Prevention System.(EPAADPS)”.EPAADPS aims to proactively detect and prevent known and unknown attacks which embodies immune attributes to distinguish self and non self to prevent novel, unseen anomalies. EPAADPS combines the principles of immunity with agents to develop a proactive anomaly detection and prevention system which not only detects an attack but also takes appropriate measures to stop it. The newly introduced self-tuning and detector power mechanism used in detector generation and selection enables EPAADPS to select self-tuned and powerful detectors in detector set. Agents accompanying detectors collaborate and communicate between themselves to proactively discover correct anomalies and then take appropriate preventive measures. Detector agents with voting mechanism collaborate and facilitate to cover self region more precisely proficiently and correctly. EPAADPS reports high detection rate, low false alarm and low detector rejection rate.

3. Comparison With Related Works

This section briefly discusses about comparison with related works. The anomaly detection system based on variable N-gram features and one class SVM is based on a novel feature extraction technique, which combines the frequency with the temporal information from system call traces and one class SVM detector. This system has the advantage of reducing false alarm rate and providing high level of detection accuracy.

The detection of anomalies in time series data via deep learning algorithm which combines wavelets, neural networks and Hilbert transform presents a new signal processing algorithm in which anomalies are detected by analysing the amplitude of the residual signal and instantaneous frequency hierarchically using probabilistic Receiver Operating Characteristics. The algorithm is fast, performs robustly and is transferrable.

The hybrid intrusion detection prevention system proposed an improvement in the framework of current host IDPS/network using signature based anomaly based methodologies by implementing a hybrid VMM-based honeypot into a theorized self-healing hybrid IDPS. This hybrid IDPS has the advantages of efficiency and accuracy.

The anomaly detection for traffic verification in sensor networks uses Gaussian mixture model for verification. Traffic which obeys the model is determined as normal or as anomaly. The system has better performance in terms of delay, throughput and packet delivery ratio and efficient in detecting anomalies.

The anomaly detection using outlier detection approach, the anomaly dataset is measured by the Neighbourhood Outlier Factor (NOF) and the proposed IDS has the advantage of less execution time and less trained datasets.

The anomaly detection in an efficient proactive artificial immune system based anomaly detection and prevention system detects anomalies using detectors and take appropriate preventive measures from further attacks. The system have high detection rate, low false alarm rate, and low detector rejection rate. EPAADPS facilitate better and correct self and non-self coverage

4. CONCLUSION

In this paper, a survey on different techniques used for detecting anomalies and the advantages of those techniques over other techniques that are previously used is presented. Also we have discussed about the comparison between those papers we have surveyed.

REFERENCES

[1] Wael Khreich ,Babak Khosravifar,Abdelwahab Hamou-Lhadj ,Chamseddine Talhi , "*An anomaly detection system based on variable N-gram features and one-class SVM*," ,Information and Software Technology 91,pp.186-197,2016.

[2] Stratis Kanarachos , Stavros-Richard G. Christopoulos, Alexander Chroneos ,Michael E. Fitzpatrick , "*Detecting anomalies in time series data via a deep learning algorithm combining wavelets, neural networks and Hilbert transform*", Expert systems with applications 85 , pp.292-304,2016.

[3] Syed Rizvi0F, Gabriel Labrador, Matt Guyan, Jeremy Savan, "*Advocating for Hybrid Intrusion Detection Prevention System and Framework Improvement*," Procedia Computer Science 95, pp.369 – 374,2016.

[4] Lalitha K V, Josna V R, "*Traffic Verification for Network Anomaly Detection in Sensor Networks*,"Procedia Technology 24, pp.1400-1405,2016.

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

[6] Praneet Saurabh, Bhupendra Verma, "*An efficient proactive artificial immune system based anomaly detection and prevention system*," Expert systems with applications 60 , pp.311-320,2016.