RESEARCH ARTICLE OPEN ACCESS

Survey on Intrusion Detection Methods

Amrata Saraswat*, Jyoti Mathur**
*(Associate Professor in Computer Science, Modi Institute of Technology,Kota
Email: amrita.saraswat@gmail.com)
** (Lecturer , Govt Ramchadra Khaitan Polytechnic College, Japur
Email: Jyoti.ce@gmail.com)

--************************----------------------------------

Abstract:

In Computer Network Management network security has been one of the most important problems. Intrusion is the most widely used for security. Now a days, intrusion detection played an important role in the field of network security. Intrusion detection system obtain better results when it identify each attacks as a individual problem and solved it by specific algorithms. Recently various method and model are available for intrusion detection. This paper will show a survey of intrusion detection. Intrusion detection method help the users to develop secure information systems and also improve the detection rate.

Keywords — **Network security ,data mining, intrusion detection system, Clustering.**

--************************----------------------------------

I. INTRODUCTION

Intrusion detection systems are devices that have been used to the wall of security for prevent malicious activity in a system. Network Intrusion detection systems(NIDS identify to detect incoming and on-going attacks on a network. Presently, commercial IDSs use a database of rules, called signatures, to try to detect attacks on a host computer or a network. An intrusion detection system is an important tool for network administrators because without such a device, it can't possible to identify the huge amount of packets those are traversing on current networks in every second. Moreover, new attacks as well as variants of known attacks can often go through the system without being detected.

The following advantage provide IDS:-

- Enforcement of use policies
- Collection of evidence
- Prevention of attacks
- Detection of policy violations
- Enforcement of connection policies
- Detection of attacks

There are following are the factors for the measurement of IDS.

➢ False alarm Or False positive (FP)- It means the number of detected attacks but it is really normal.

➢ False negative (FN)- It means to the number of detected normal in other words these attacks are the goal of intrusion detection systems.

➢ True positive (TP)- It means to the number of detected attacks and it is in true attack.

➢ True negative (TN)- It means to the number of detected normal instances and it is normal.

II. Survey on Intrusion Detection System Using Different Approach

INTRUSION DETECTION METHODS

There are various methods of Intrusion Detection methods as state full pattern matching, protocol decode-based analysis ,pattern matching etc .

There are following methods :

1) ***Full Pattern Matching:***

In this method signature development adds to the pattern match the concept that because a network stream has more than single atomic packets, matches should be made in context within the state of the stream. In other words systems that perform this type of signature analysis must consider arrival order of packets in a TCP stream and should handle matching patterns across packet boundaries [5].

2) ***Protocol Decode-Based Analysis:***

. In This signature is implemented by decoding the various elements in the same manner as the client or server in the conversation would. When the protocol are identified, the IDS apply rules that is defined by the RFCs to look for violations. In many cases, these violations are found with pattern matches within a specific protocol field and some require more advanced techniques that identify such variables as the number of arguments or the length of a field.

3) ***Pattern Matching:***

It is based on searching a fixed sequence of bytes in a single packet. it is a method that is fairly rigid but simple to employ. Generally the pattern is matched only if the suspect packet is associated with a particular service or destined to/from a particular port [3, 4]. The structure of a signature based on the simple pattern-matching work if the packet is IPv4 and TCP and the destination port is 2222 and the payload contains the string "foo," fire an alarm.

4) ***FUZZY CLUSTERING FOR IDS:***

The aim of fuzzy clustering method is to separate a given set of information into clusters .After that fuzzy clustering module, the training set is clustered into several subsets. Then details that the size and difficulty of every training subset is reduced. There are two types of clustering techniques hard clustering techniques and soft clustering techniques. Towards partition of training set, we also require to aggregate the outcome for fuzzy aggregation module. So, we opt the soft clustering method for fuzzy clustering module [6, 7]..

III ***Data Mining Techniques for Intrusion detection Survey [15]***

Data mining is used to examine large amount of network data. Different Data Mining techniques like clustering, classification and association rules are proving to be useful for analyzing network traffic. There are following steps:

- Data cleaning -to remove irrelevant data
- Data integration -In this step multiple data sources may be integrated.
- Data selection- From this step select the data that is necessary for analysis
- Data transformation -In this step data are transformed into appropriate forms for mining by some function as summary or aggregation.
- Data mining -It is an essential step where intelligent methods are applied for extract data pattern.
- Pattern evaluation- In this step identify the patterns representing knowledge based on some essential features.
- Knowledge presentation -Here visualization techniques and knowledge representation are used to present the mined knowledge to the used.

Data Mining is used in different application that requires data analysis. Presently data mining techniques plays an important role in intrusion detection systems. Different data mining techniques like Classification, Clustering and Association rules are frequently used for information about intrusions by observing network data.

A. Association-

It is mostly used for a transaction data analysis. Associative classification consist of one method as classification. consists of two steps. In the first step , using a modified version of the standard association rule mining algorithm create association instructions.

In next step generate a classifier with the help of the association rules.

B. Classification

Classification method can be useful for both misuse detection and anomaly detection, but it is mostly used for misuse detection. It is the method for finding a set of functions that describe data classes for the purpose of being able to use the model to find the class of objects whose class label is not known. This model depends on the a set of training data information (i.e. The derived model may be show in different forms like decision trees, neural networks and classification rules,. It has following:

- **Decision Trees:** It is a tree structure, where each node show an attribute value, each branch show an outcome of a test, and tree leaves represent classes. Decision trees can be easily use the classification rules. Decision trees are smaller size trees and easy to interpret.

- **Rule-Based Classification:** It represent in the form of If-Then rules. In this a rule is find as per the accuracy and coverage of the classifier. If we find more than one rule then we need to conflict resolution in rule-based classification. Conflict resolution can be solved with three different factors as Class-Based ordering, rule-based ordering and Size ordering. Rules are easy to understand. Each leaf holds the class prediction.

- **Frequent-Pattern Based Classification:** It is used for finding the most frequent and relevant patterns in bulk of datasets. Frequent patterns are as subsets that present in a data set with a frequency no less than a user-specified.

- **Rough Set Theory:** It can be used for find the structural relationships within noisy data. It use the discrete-valued. This theory is based on the settlement of equivalence classes within the given set of data. All the data samples have a similarity class. So, the samples are equal having the same attributes. It can also be used for feature reduction and relevance analysis.

C. Clustering

It can be applied on both Anomaly detection and Misuse detection. This paper presents basic steps involved in identifying intrusion are follows:-

Search the largest cluster which has maximum number of instances and mark it as normal.

Then arrange the rest clusters in an ascending order of their distances.

- Select the first K1 clusters so that these

clusters sum up to ¼`N, and name them as normal

- Mark all other clusters as malicious.

- After clustering, heuristics are used to automatically to mark each cluster as either normal or malicious.

I IV Implementation of Intrusion Detection System by Data Mining Algorithm [16]

In recent years Internet technology has developed and both hardware and software system have improved. Internet brings people not only great potential threats but also convenience.

Data Mining find the understandable pattern from a large incomplete, noise, non-stable , the process of extracting effective, updated, latent, useful, and random data. intrusion detection system deals from multiple sources like, system logs, application , network traffic ,warning alarm etc. Due to various data source and format, the complexity increased in analysis of data. Data Mining has the most advantage in data extraction from huge amount of data that are noisy and dynamic. Data mining can find useful knowledge from a bulk of data. There are following advantages of applying data mining to an intrusion detection system -

1) It can be used to construct an intrusion detection system in various computing environments because of mechanical mess and universality of mining process itself and the system can generate good quality of detection model from a bulk of audit data to overcome artificial intervention .

2) Presently, development of data mining technology has got a large number of algorithms from the fields, like, , database machine learning, statistics and pattern recognition etc and some algorithms are specially useful for intrusion

detection, like cluster analysis, classification analysis and sequential pattern analysis, association rule analysis etc, In the previous papers show that applying these technologies to intrusion detection is feasible and effective.

V Intrusion Detection based on K-Means Clustering and One R searching[17]

In this method KM+1R, combines with the OneR searching technique. The k-means clustering and research publications based on hybrid [11], false positive (FP), true positive (TP), false alarm (FA), The detection rate (DR), false negative (FN) and accuracy for each approach are also found. Each approach has strengths and weakness. Some approaches have strength in detection but high in false alarm. in [13] the author present a new three-level decision tree classification, which has the detection rate. In intrusion detection a number of hybrid techniques have been presented.

The main goal to utilize K-Means clustering method is to group data and to split into normal and attack instances. K- Means clustering methods divide the input dataset into k- clusters according to an initial value and the centroids is the mean value of numerical data contained within each cluster .

There are following steps:

1. Select initial centers of the K clusters..
2. Generate a new partition by assigning each data to its closest cluster centers.
3. Compute new clusters as the centroids of the clusters.

One-R algorithm select attribute with lowest error rate . There are following Steps:

1. From clustered set, create a rule set for each value of each attribute as in step i, ii, iii and iv.

i. Count each value of target class appears.

ii. Search the most frequent class.

iii. Make a rule set assign that class to this value of attribute predictor.

iv. Find the total error occurs in the rules set for each attribute predictor.

v. Select the best attribute which have a smallest total error and this as a classification rules.

VI Intrusion Detection Method Based on Improved DBSCAN [18]

In clustering analysis algorithm of data mining DBSCAN is a very useful method. DBSCAN means “Density-Based Spatial Clustering of Application with Noise”. This is useful for solving problem as points crowded.It has so many neighbours near it. DBSCAN find them and place them in clusters. DBSCAN has two parameter ∑ — defines the size and borders of each neighborhood. The ∑ is a radius. the ∑-neighborhood of x, is the circle/ball with radius ε around point x.Experiment results prove this method for reduces the false negative rate and promotes the performance of intrusion detection system,

➢ Traditional DBSCAN algorithm for intrusion detection is used by author et al. [10]. It generates a cluster and merge some small clusters. This paper present a density-based clustering algorithm for intrusion detection.It also use rational method for calculating the distance and the merging process is optimized[8]. It also help for selection of parameter.

➢ When DBSCAN algorithm is used to find intrusion data that time small clusters are generated at the time of experiment results. These small clusters contains number of records more than 70% having a high false alarm rate. These small clusters are nearest to normal clusters. For solve such type of problem [10] proposed IDBC (Improved Density Based Clustering Algorithm) for merging some small clusters. During merging process calculation has been find out between two clusters.

VII A Graph –based clustering algorithm for anomaly intrusion detection[19]

A graph based approach is presented by Zhou Mingqiang et al [20] .In this method intrusion detection algorithm by using outlier detection method that based on local deviation coefficient (LDCGB). It is Compared with other intrusion detection algorithm of clustering, this algorithm is unnecessary to initial cluster number. Meanwhile, it is robust in the outlier's affection and able to detect any shape of cluster rather that the circle one only. Moreover, it still has stable rate of detection on unknown or muted attacks..

s. no.	Author	Accuracy	False Positive rate	Detection Rate	False negative rate
1	Z. Muda, W. Yassin	Yes	Yes	Yes	No
2	DeepthyK Denatious & 2Anita John	Yes	No	Yes	No
3	Changxin Song, Ke Ma	Yes	No	Yes	No
4	LiTian1, Wang Jianwen1	Yes	Yes	Yes	No
5	Sanoop Mallissery et. al.	Yes	No	Yes	No
6	Li Xue-yong, Gao Guo	Yes	Yes	Yes	No
7	Zhou Mingqiang et. al.	Yes	No	Yes	No

CONCLUSION

Detection of intrusion attack play an important role in network security system. Different approaches help us for reducing losses of attack, find out abnormal attack and enhancing system security. This paper gives awareness of network security.

FUTURE WORK

With my experience in during working in different approaches, we found out that in future we will work on use *of* intrusion detection in fog computing and IDS for wireless sensor network. we will also compare result with previous research and find out better result in accuracy, failure analysis rate and false alarm.

REFERENCES

[1] Giovanni Vigna ,Christopher Kruegel and Fredrik Valeur. "Intrusion Detection and Correlation: Challenges and Solutions", volume 14 of Advances in Information Security. Springer- Verlag, 2005

[2] " Intrusion detection: A brief history and overview",IEEE Security and Privacy, by Giovanni Vigna in April 2002

[3] Eugene H.Spat'tord, Sandeep Kumar "An Application of Pattern Matching in Intrusion Detection", Technical Report 94-0 13, Department of © 20 1 1 lET 228 Computer Sciences, Purdue University, West Lafayette, March 2004.

[4] "A Pattern Matching Model for Misuse Intrusion Detection", The COAST Project, Department of Computer Sciences, Purdue University, West Lafayette, by Eugene H.Spat'tord, Sandeep Kumar in 47907- 1 398.

[5] "Flexible Pattern Matching in Strings", by Gonzalo Navarro, Mathieu Raffinot, Cambridge University Press 2002, ISBN 0-52 1-8 13077.

[6] Jukka Juslin, John E. Dickerson, Ourania Koukousoula, Julie A. Dickerson, "Fuzzy Intrusion Detection", Electrical and Computer Engineering Department, Iowa State University, Ames, lA, USA.

[7] "Mining Fuzzy Association Rules", by K.e.C.Chan and W.H.Au, Proc.Of ACM CIKM, 1997, pp.209- 2 15.

[8] "Computer Security Threat Monitoring and Surveillance", Fort Washington, PA,by Spector, James P Anderson, in 1980.

[9] "Intelligent Data Mining and Knowledge Discovery", b y JIAO Licheng Jiao, Fang Liu, and Jing Liu Xi'an: Xidian University Press,2006,pp.325-326.

[10] "An Improved Intrusion Detection Algorithm Based on DBSCAN", by Yang Jian, Micro Computer Information, 25,1008- 0570(2009)01- 3-0058-03, 58-60,2009.

[11] "Design of multiple level hybrid classifierfor intrusion detection system using bayesian clustering and decision tree", Pattern Recognition by C. Xiang, P.C. Yong, L.S. Meng, Letters 29 918-924,2008.

[12] "Survey on intrusion detection method",2011 by Sanoop Mallissery , Jeevan Prabhu,and Raghavendra Ganiga,.

[13] "Survey on Data Mining Techniques to Enhance Intrusion Detection", by Deepthy K Denatious & 2Anita John, in 2012.

[14] , Ke Ma Institute of Computer Information & Technology of Qinghai Normal University Network Center of Qinghai Normal University Qinghai, China.,by Changxin Song on topic "Design of Intrusion Detection System Based on Data Mining Algorithm",2009.

[15] Department of Computer Science, North China Electric Power University (NCEPU), Baoding 071003, China, "Research on Network Intrusion Detection System Based on Improved K-means Clustering Algorithm", by Li Tian1, Wang Jianwen1 2009

[16] "A New Intrusion Detection Method Based on Improved DBSCAN", by Li Xue-yong, Gao Guo- in 2010.

[17] "A Graph-based Clustering Algorithm for Anomaly Intrusion Detection", 2012 by Zhou Mingqiang,HuangHui,WangQian,