A Novel Approach to Measure the Quality of Cluster and Finding Intrusions Using Intrusion Unearthing and Probability Clomp Algorithm

Azhagiri. M
Computer Science Engineering
St. Peters University
Avadi, Chennai, India

ABSTRACT: Objectives: *Network security is used to monitor and prevent unauthorized access, deployment, enhancement, or contradiction of a network of computers. Network security is a primary issue in processing on the grounds that numerous assortments of assaults are expanding step by step. Despite the fact that, more number of research works were completed in the past for system security yet at the same time there are numerous testing issues.*

Methods/Statistical Analysis: *To address the issues in the existing literature, the probability clomp algorithm has been proposed to form the cluster and intrusion unearthing algorithm has been implemented among the clustering environment.*

Findings: *The execution of the proposed Intrusion Detection System (IDS) recognizes the interruption significantly more successfully than the current frameworks. The quality of the cluster is measured with the help of attributes like precision and entropy which is compared with the existing approach.*

Application/Improvements: *The proposed algorithm is able to achieve high observations and detection to overcome the disadvantages of existing algorithm.*

Keywords: Intrusion Detection System, Network Security, Clusters, KDD, Intrusion Unearthing Algorithm And NSSA

Received: 24 November 2017, Revised 23 December 2017, Accepted 9 January 2018

DOI: 10.6025/isej/2018/5/1/11-23

1. Introduction

Network security consists of the provisions and strategies adopted by a network administrator to supervise and frustrate unauthorized access, utilization, amendment, or refutation of a computer network and network-accessible resources. Network security is considered to be more decisive because of inventive property that can be effortlessly acquired through the network. The confidentiality and the integrity are significant and are to be considered for embryonic a secure network[1]. It must endorse that the non-authenticated party does not audit the data and also it must guarantee that the data which is received has not been altered.

Network Security Situational Awareness (NSSA) is a rising technique within the field of network security and it helps security analysts to be conscious of the fastidious security scenario of their networks. NSSA has been a hot analysis within the network security domain. Intrusions are the activities that infringe the security policy of the system. The general attacks on the networks are DoS, U2R, R2L and probe. Intrusion Detection System (IDS) is a device; typically another separate computer that monitors the activity to recognize these attacks malicious or suspicious events and IDS monitors the system and user activities. It audits the system configuration vulnerabilities and misconfigurations. It corrects the system configuration errors. Intrusion detection rate and interference detection rate are the same. Each is used to observe the bug that enters in our network or host. The distinction is that the interference system can offer the response to bug by firewall, anti-spam and by interference through the malicious activity. So, it is required to perform the intrusion detection in network and host. There are 2 styles of intrusion detection system which are signature based and anomaly based detection methods. The KDD CUP 1999 data set contains a standard set of data to be audited which contains a diversity of instructions simulated in a military environment. In our proposed work the KDD cup 1999 data set is grouped into clusters using probability clomp clustering algorithm. This algorithm doesn't provide single partitioning data set but instead provides extensive hierarchy of clusters that merge each other at certain distance[3].To avoid intrusion in the cluster, the intrusion unearthing algorithm is used.

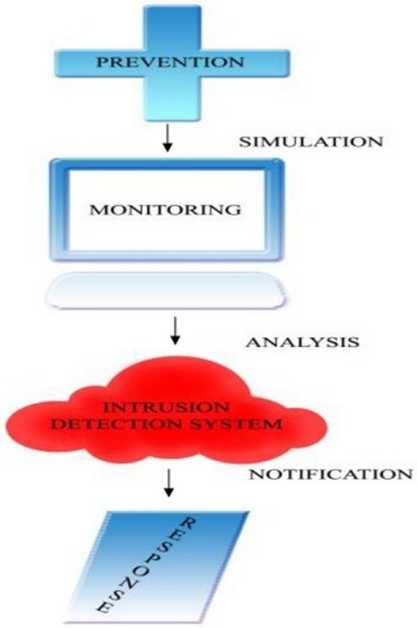

Figure 1. Architecture of IDS

The above figure shows the general architecture of IDS in which how the functions are carried out. IDS is a device, typically another separate computer that monitors the activity to identify these attacks, malicious or suspicious events. The IDS monitors the system and user activities as shown in figure 1. It audits the system configuration vulnerabilities and misconfigurations and accesses the correctness of data file. IDS detect the abnormal activity through statistical analysis which corrects the system configuration errors. The intrusion detection is performed at network and host level. The anomaly based IDS will monitor the network traffic and compare it against an established baseline in which the rules and criteria are satisfied or not. The signature based IDS system will monitor the network traffic and compare it against a database of signature from suspicious threads.

The organization of the paper is as follows. Section 2 describes the related work. Section 3 deals with the KDD cup data set. The proposed architecture of intrusion detection system is described in section 4. Section 5 represents the results analysis and comparison with the existing system. The conclusion of the proposed work is explained in the section 4.

.

2. Related Work

The intrusion detection system is the system to seek out the intruders in networks. In [1]have proposed assorted IDS models and

techniques. In this paper, both the signature based and anomaly based IDS were used for intrusion detection system. Anomaly based IDS finds the anomalies based on the rules described in it. The author did not address the cluster and its quality through which the intrusion is detected.

In [2]have proposed the fuzzy genetic algorithmic program which achieved the better detection rate than a decision tree algorithmic program in most cases, and it absolutely as shrewd at detecting unsolved attacks. The genetic algorithmic program had a high detection rate for denial of service attacks. When compared with the winning entry of the KDD cup 99 Classifier Learning Contest, it was shown that it possesses a more robust detection rate for each denial of service and user to root attacks. The author claimed that utilizing of fuzzy genetic algorithms in intrusion detection will efficiently detect the attacks. Proposed algorithm lacks to achieve efficiency at 95%. The author did not claim that the clustering approach to seek out the intrusion in networks.

In [3]have proposed the anomaly based intrusion detection system for detecting the intrusion behavior within a computer network. A fuzzy decision-making module was designed to build the efficient system using fuzzy rules. At first, definite rules were generated by mining the frequent things from attack knowledge using traditional knowledge. Then, fuzzy rules were known by fuzzifying the definite rules and these rules got to fuzzy system, the classifications based on the knowledge. The author claimed the work at design level and not in the implementation level. We have used KDD cup 99 dataset for evaluating the performance of the proposed system and the experimentation results showed that the projected technique is effective in detecting numerous intrusions in computer networks.

The two data mining techniques and anomaly detection algorithms were implemented [4]. A random forest classification algorithm is utilized in misused detection part. Weighted k-means clustering algorithm was used to cluster the data. Random forest is a powerful algorithm for building the patterns automatically instead of coding rules manually. The proposed approaches are evaluated over 10% KDD'99 dataset. In misuse detection framework, intrusion patterns are built in the offline phase.

In [5]they have discussed the intrusion detection algorithm. In this algorithm decision stumps and online GMMs were used as weak classifiers for the traditional online Adaboost and for the proposed online Adaboost. The results of the algorithm were compared with the results of the algorithm using online GMMs and the proposed online Adaboost. A distributed intrusion detection framework is also proposed in addition. The proposed work overcomes the difficulties in handling the mixed-attributes of network connection data. The local parameterized detection models were suitable for information sharing: among nodes only a very small number of data is shared.

In [6] the importance of intrusion detection (IDS) system has been discussed. Its function can be divided two parts, outer intrusion detection and inner illegal host's detection and prevention. To detect intrusions from the Internet a novel methods GNG, a clustering methods Principal Components Analysis and Self Organizing Map (PCASOM) are integrated. The simulation explains that the IIDS system can obtain obviously better performance than single method.

In [7]they have analysed the importance of designing appropriate intrusion detection systems to combat attacks against cognitive radio networks and also an effective IDS, which can be easily implemented in the secondary users' cognitive radio software. The proposed IDS use a non-parametriccusum algorithm, which offers anomaly detection. In particular, the authors presented an example of a jamming attack against a CRN secondary user, and demonstrated how the proposed IDS is able to detect the attack with low detection latency.

In [8] they have explored the essentials of intrusion detection in a Gaussian distributed WSN by characterizing intrusion detection probability with respect to intrusion distance and network deployment parameters. The network deployment parameters are intruder's starting point, deployment point, deployment deviation, number of deployed sensor and sensing range. Two detection models are considered from the research, single-sensing detection and multiple sensing detection. This work allows to analytically formulating the intrusion detection probability within a certain intrusion distance.

In [9] they have described about the intelligent system to maximize the recognition rate of network attacks by embedding the temporal behaviour of the attacks into a neural network structure. The proposed system consists of five modules: packet capture engine, pre-processor, pattern recognition, classification, and monitoring and alert module. These modules were tested in a real environment where it has shown good capability in detecting attacks. In addition, the system has been tested using DARPA 1998 dataset with 100% recognition rate. The proposed system can recognize attacks in a constant time.

The author used only small part of data from the data set for testing.

In [10] they have used Arduino simulator for intrusion attack. Using this simulator several attacks were carried out and noted the different detection times. To evaluate these detection times the same simulator has been used in the attacks on the same network and in the same conditions. The detection times of the software IDS are compared with the standalone IDS. From the experiment, the standalone IDS response times is better than the software IDS. This paper described about the intrusion finding method which was implemented by simulator and not by the original data set.

In [11] they have combined two methods of clustering and optimization, namely K-means and Simulated Annealing, in order to achieve a global optimum classification for the data subject to learning. The K-Means algorithm used in its semi-supervised variant in order to lessen the number of times that the algorithm is applied. The developed algorithm has produced satisfactory results when applied on NSL-KDD data set, the tests reveal this method can enhance the detection and misdetection rates of intrusion detection systems. The author did not address the quality of the clusters. The proposed work of this paper is not able to predict the quantification percentage.

In [12] they suggested a hybrid method of Support Vector Machine (SVM) as well as Genetic Algorithm (GA). The proposed methods are used for reducing the number of features from 41 to 11 using KDD Cup'99 dataset. The features are classified as three priorities using GA with the most significant as the first priority and the least one as the third priority. The way in which feature distribution is done is that four features are placed in the first priority, five in the second and two in the third. The results show that the suggested hybrid algorithms, GA and SVM are able to achieve true and false positive values of 0.973 and 0.017 respectively.

In [13] they proposed a new variant of Principal Component Analysis (PCA) called PCA Lp-norm using conjugate gradient algorithm to solve the Lp-norm optimization problem. The main idea behind this new method relies on the Lp-norm, which is more robust to the presence of outliers in data. Extensive experiments on two well-known datasets namely KDDcup99 and NSL-KDD prove the effectiveness of the proposed approach in terms of network attacks detection, false alarms reduction and CPU time minimization.

2.1 Discussion

More number of issues was addressed in the past literature but the quantification of the system is very limited. The clustering approach is also not addressed in the related work.

3. KDD CUP 1999 Data Set

The KDD cup 1999 data set is used for the intrusion unearthing methods. This data set contains a standard set of data to be audited which contains a different types of instructions simulated in a military environment. It contains 4GB of compressed raw data of seven weeks of network traffic. It consists of two million connection records. With this data set, the data can be distinguished either as attack or normal. It contains 494,019 records. Each record has 41 attributes and named as attack and normal. One of the disadvantages in this data set is the large number of repetitious records. It is found that about 75% - 78% of the records are duplicated in the test set and train set respectively. To avoid intrusion the KDD cup 1999 data set is grouped into clusters using Probability Clomp Algorithm (ProCA)..

This algorithm does not provide single partitioning data set but instead provide extensive hierarchy of clusters that merge each other at certain distance and avoids the duplications to a greater extent.

3.1 Intrusion Detection Systems

Intrusion detection systems are used to identify the malicious or suspicious events intrusions as the activities that violate the security policy of the system. The general attacks on the networks are DoS, U2R, R2L and probe.

Denial of service attack (Dos)

In this attack, the intruders make the memory too full and busy to handle the requests.

User to Root Attack (U2R)

In this attack, the intruder's attempts to access the user account.

Remote to Local Attack (R2L)
In this attack, the intruders sends packet to a machine over a network but does not have an account on that machine.

Probing Attack
In this attack, the intruders attempts to gather data about the network of computers.

4. Architecture of Intrusion Detection System

The proposed work involves grouping of KDD cup 1999 data set into clusters using PCA. Each cluster will have a cluster head namely Head 1, Head 2,.,.Head n. To avoid intrusion in the cluster, the intrusion unearthing algorithm is used. The algorithm gives a notification as Yes or No to indicate whether there is an attack or not. The intrusion detection rate in our proposed system is better than the existing systems. The experimental result shows that the proposed system achieves higher accuracy.

4.1 Description
Initially user query has been collected and checked with the related data set which forms the cluster using the proposed Probability Clomp Algorithm (ProCA) which is described in the figure 2. This algorithm creates a cluster head for each cluster through which the query can be accessed. In this clustering a new algorithm namely Intrusion Unearthing Algorithm 1 and 2 has been implemented to identify the intrusion in the cluster. This proposed algorithm finds the intrusion, if found it gives notification to the user. Otherwise it displays the message no intrusion is found at current run.

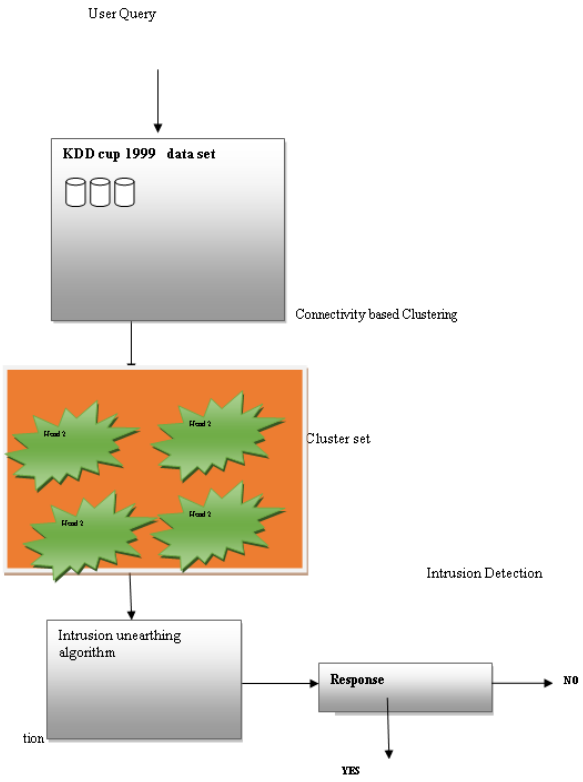

Figure 2. Architecture of IDS

Each run this proposed algorithm is invoked and gives the response through which the percentage of intrusion present in the cluster is measured.

4.2 Probability Clomp Algorithm (ProCA)
It deals with the clustering of data in the dataset. Primarily, the related data is collected and formed to a cluster. Each cluster has cluster head through which the data is communicated. The election algorithm is invoked to form the cluster head.

Input: KDD Data set

Output: Formation of cluster head and cluster

Procedure

1: Begin

2: while (dataset !=Null)

3: Begin

//Divides the data set n number of groups

4: If (dataset = =10 MB)

5: Name it as d1

6: Repeat step 4 until empty

7: Else

8: Print" dataset is empty"

9: End

10: Call election algorithm to form cluster head

Input: Clusters

Output: Formation of cluster head

1: Begin

2: A = variable to verify the threshold on the cluster-head's head1;

3: If (A is false) Then

do not perform Cluster-Head re-election;

4: Else

5: Cluster-Head election is called;

All the Member nodes participate in the election Procedure

4.3 Intrusion Unearthing Algorithm (IUA1)

The IUA1 describes to find the intrusion in the data set. Generally IDS has two algorithms namely IUA1 & IUA2 acts as a two step verification in the data set.

Input: Non-Categorical Attributes $C_1, C_2, .., C_n$

Output: Decision Tree

//The **IUA1** algorithm is used to build a decision tree, given a set of non-categorical attributes $C_1, C_2, .., C_n$, the categorical attribute C, and a training set T of records.

Description:

function **IUA1** (R_c: A set of non-categorical attributes,

C: The categorical attribute,

T: A training set)

returns a decision tree;

1: Begin

2: If T is empty

3: Return a single node with value Failure;

4: else

5: If (T != $NULL$) // consists of records all with the same value for the categorical attribute,

6: return a single node with that value;

7: else

8: If ($R == NULL$)

9: $T_1 = M_{sr}$ // return a single node with as value the most frequent of the values of the categorical attribute that are found in records of T;

//[note that then there will be errors, that is, records that will be improperly classified];

10: End

11: End

12: $D = (D, T)$// attribute with largest Gain among attributes in R_c;

13: $[D_j| = D$ // where $j = 1,2, .., m\}$ be the values of attribute D;

14: $[T_j| = T$// where $j = 1,2, .., m\}$ be the subsets of S consisting respectively of records with value D_j for attribute D;

15: Return a tree with root labeled D and arcs labelled $d_1, d_2, .., d_m$ going respectively to the trees

IUA1(R_c-{D}, C, T_1), **IUA1**(R-{D}, C, T_2), .., **IUA1**(R_c-{D}, C, T_m);

16: end **IUA1**;

Advantages of Algorithm

a. From the training data set easy prediction rules can be generated.

b. It builds the short tree and fastest tree.

c. Understandable prediction rules are created from the training data.

d. Builds the fastest tree.

e. Builds a short tree.

f. Only need to test enough attributes until all data is classified.

g. Finding leaf nodes enables test data to be pruned, reducing number of tests.

4.4 Intrusion Unearthing Algorithm (IUA2)

The decision trees generated by IUA1 can be used for classification, and so IUA1 is often referred to as a statistical classifier. It builds decision trees from a set of training data using information theory concept. An attribute that mostly divide the samples into subsets are chosen by IUA1. The dividing criterion uses the information gain. To make decision the attribute with the highest information is selected.

Procedure

Input: Training dataset T; attributes C.
Output: Decision Tree.

1: Begin

2: If ($T == NULL$) then

3: Return failure

4: End if

5: If ($C == NULL$) then

6: Return Tree as a single node with most frequent class label in T

7: End if

8: If ($C_1 = 1$) then

9: Return Tree as a single node C

10: End if

11: Set Tree = {}

12: For every C do

13: Set Info(a, T) = 0

14: SplitInfo(a, T) = 0

15: Compute Entropy(a)

16: For every values(a, T) do

17: Set $T_{a,v}$ as the subset of T with attribute $a = v$

18: Info (a, T) += $\frac{|T_{a,v}|}{|T_a|}$ Entropy(a_v)

19: *SplitInfo* (a, T) += $\frac{|T_{a,v}|}{|T_a|} \log \frac{|T_{a,v}|}{|T_a|}$

20: End for

21: Gain (a, T) = Entropy (a) - info(a, T)

22: End for

23: GainRatio (a, T) = Gain(a, T) / *SplitInfo* (a, T)

24: Set a_{best} = argmax{GainRatio(a, T)}

Attach a_{best} into Tree

25: For every values(a_{best} , T)do

Call IUA1($T_{a,v}$)

26: End for

27: Return Tree

The input for the algorithm consists of a set S of examples described by continuous or discrete attributes, each example belonging to one class.

The output is a decision tree or/and a set of rules that assigns a class to a new case.

The information gain by a training dataset T is defined as:

$$Info(a, T) += \frac{|T_{a,v}|}{|T_a|} Entropy(a_v)$$

The information gain ratio is calculated as Gain(a, T) = Gain(a, T) / SplitInfo(a, T)

Where the split information is calculated as

$$SplitInfo\ (a, T) + = = -\frac{|T_{a,v}|}{|T_a|} log \frac{|T_{a,v}|}{|T_a|}$$

5. Result Analysis

The sample KDD data set has been taken for verifying the intruders in the cluster. The related data are grouped and formed as clusters. Each cluster has one head through which the information is retrieved. The following figure shows the values of the precision and recall parameters of the clusters in each run of the data set using the formulas from 1 to 4. The blue colour shows the precision values for the increasing of the data set and the other colour represents the recall values of the increasing data set.

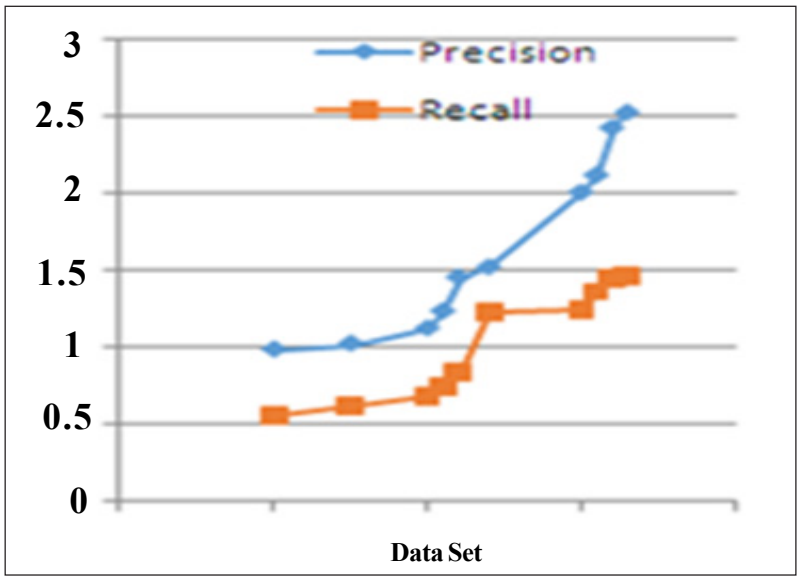

Figure 3. Data set versus precision and recall values for proposed method

5.1 Implementation of Existing Method

Using KDD data set, normal clustering approaches has been used and the precision, recall values are calculated which is compared with the proposed work.

5.2 Calculation of Precision and Recall Values for Existing Method

The Precision and Recall values are calculated for the existing approach. The existing approach is normal IDS system in which its performance is shown in figure 4.

5.3 Comparison of Existing Method and Proposed Method

The precision and recall values are calculated and compared as shown in the figure 5 and 6. The proposed values are less than the existing values.

5.4 Evaluation Index

To evaluate the capability of proposed model, we adopt following statistics measures as the
C1.Test standard

Accuracy

Accuracy is the nearness of measurement results to the true value.

Accuracy = number of correct judged classified sample / number of total sample

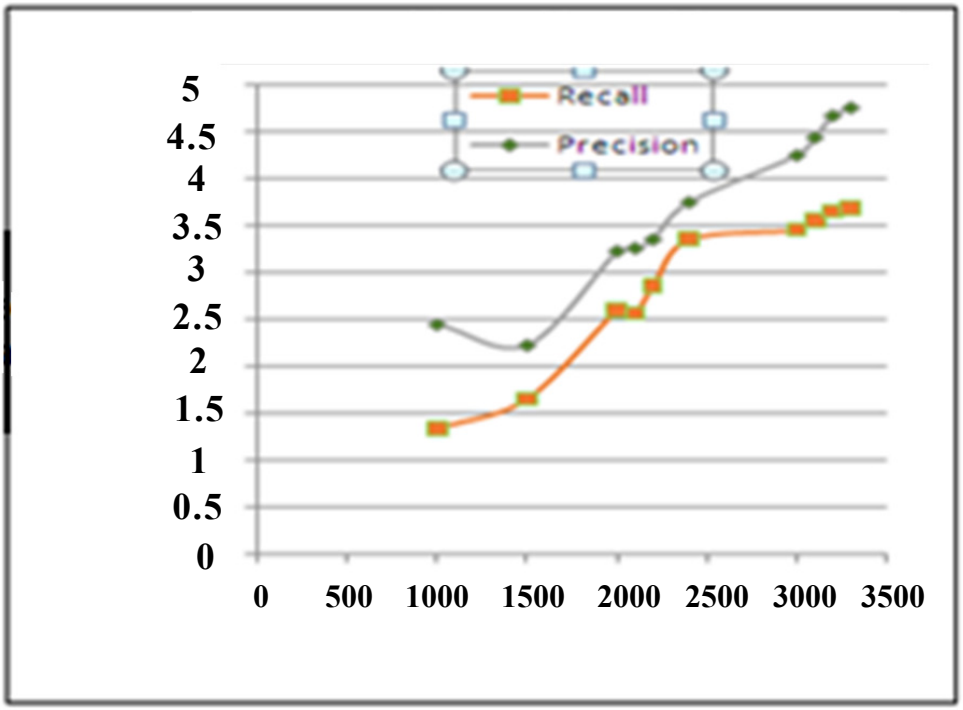

Figure 5. Comparison of Precision values for Existing method and Proposed method

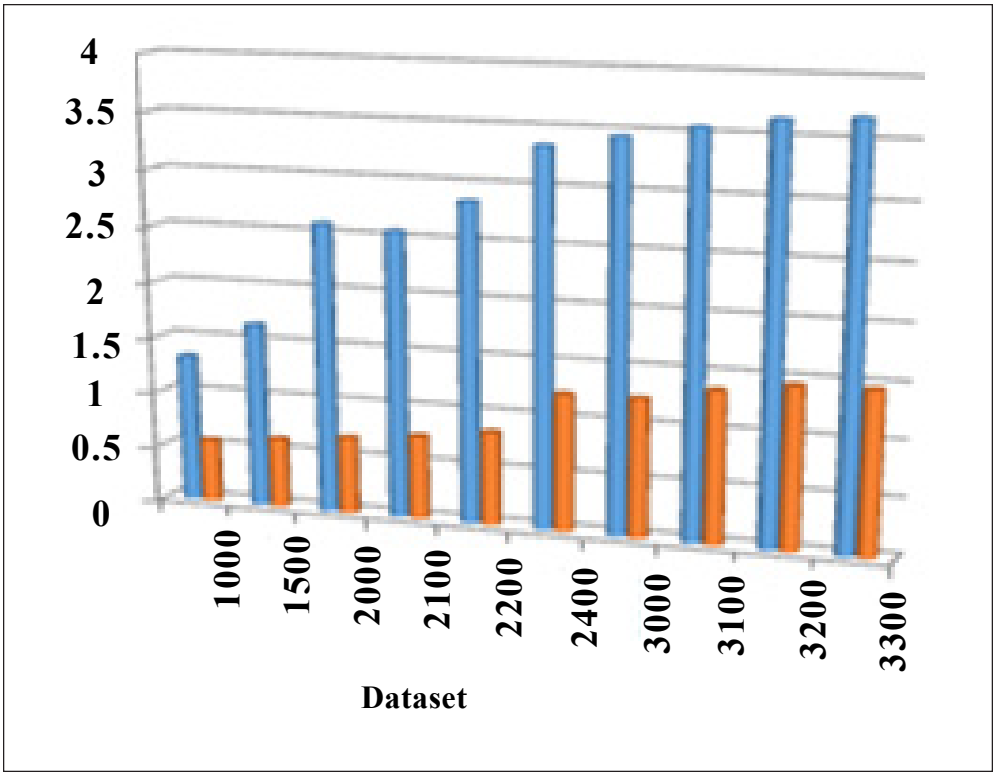

Figure 6. Comparison of Recall values for Existing method and proposed method

$$Acc = \frac{cl.s1}{s} \quad (1)$$

Precision

Precision is measured as the fraction of pairs correctly put in the same cluster.

Precision = true positives/ (true positives + false positives)

$$\text{Precision} = \frac{T.Po}{(T.Po + F.Po)} \quad (2)$$

Recall

Recall is calculated as the fraction of actual pairs that were identified.

Recall = true positives/ (true positives+ false negatives)

$$Re = \frac{T.Po}{(T.Po + F.Ne)} \quad (3)$$

F- Measure

A measure that combines precision and recall and is the harmonic mean of precision and recall, the traditional f-measure or balance f-score

F = 2* (Precision .recall)/ (precision + recall)

$$F = 2^* (Pre.\ Re)/ (Pre + Re) \quad (4)$$

Detection rate

Detection rate is the number of intrusion or true positive detected by the system.

Detection rate = number of correctly detected intrusion / number of total intrusion in test sets;

Mean, variance and standard deviation are calculated for precision for existing and proposed system. The degree of freedom is calculated for IBA, ($n1$+$n2$ - 2). 10 + 10 – 2 = 18. At 18th degrees of freedom the tabulated value is 3.92 at p = 0.001 in [11]. The calculated value is greater than the tabulated value. So, there is a 98% significant difference with the existing system.

Similarly, Mean, variance and standard deviation are calculated using the 1, 2, 3,4 and 5 formula to recall for both proposed and existing system.

Mean

$\overline{x}$ = 1.01

Variance

s^2d = 0.113

Standard Deviation

False Alarm Rate

It is defined as the normal pattern mistaken for abnormal pattern divided by the total number of normal patterns.

False alarm rate = Number of normal pattern classified as attacks / Number of total normal patterns;

T-Test

The Student's T-test has been conducted for comparing existing approach with the proposed approach.

Mean, variance and standard deviation are calculated using he following formula for precision for both proposed and existing

system.

Mean

$$\bar{x} = \sum \frac{x}{n} = 1.641 \quad (1)$$

Variance

$$\sigma^2 d = \frac{\sum (x_i - \bar{x})^2}{n} = 0.3054 \quad (2)$$

Standard Deviation

$$S.D = \sqrt{\sigma^2 d} = 0.5526 \quad (3)$$

$$\sigma^2 d = \sigma_1^2 / n_1 + \sigma_1^2 / n_2 = 0.10164 \quad (4)$$

$$\text{S.D} = \sqrt{\sigma^2 d} = 0.3188$$

Coefficient of Variance

$$CV = \frac{\overline{x1}}{SD} - \overline{x2} = 19.56 \quad (5)$$

$$\text{S.D} = \sqrt{\sigma^2 d} = 0.333$$

$$\sigma^2 d = \sigma_1^2 / n_1 + \sigma_1^2 / n_2 = 0.0725$$

$$CV = \frac{\overline{x1}}{SD} - \overline{x2} = 6.059$$

The tabulated value is 3.92 at p = 0.001in [11]. The calculated value is greater than the tabulated value. So, there is a 98% significant difference with the existing system tabulated value is 3.92 at p = 0.001in [11]. The calculated value is greater than the tabulated value. So, there is a 98% significant difference with the existing system.

6. Conclusion

Network security is considered to be more important because of inventive property that can be easily obtained through the network. The confidentiality and the integrity are needed to be considered for developing a secure network. In this paper, a detailed survey has been taken regarding the intrusion technique used in the literature. A probability clomp algorithm is applied to form the cluster and intrusion unearthing algorithms are proposed to find the intrusion among the clusters. The intrusions are avoided in the given data set in a high rate. The result of our integrated system will effectively and efficiently notice attacks. The quantification of the cluster is measured with the various metrics. The proposed algorithm is 98% significant difference with the existing approach.

References

[1] Kshirsagar, Vivek K., Tidk, Sonali M., Vishnu, Swati. (2014). Intrusion Detection System using Genetic Algorithm and Data Mining: An Overview, *International Journal of Computer Science and Informatics*, 1 (4) 2231 –5292.

[2] Emma Ireland. (2014). *Intrusion Detection with Genetic Algorithms and Fuzzy Logic Journal of Intrusion in network*, 3 (5) 1-10.

[3] Shanmugavadivu, R., Nagarajan, N. (2015). Network Intrusion Detection System Using Fuzzy Logic, *Indian Journal of Computer Science and Engineering (IJCSE)*, 2 (1) 01-111.

[4] Prathibha, K S., Pankaj Kumar., Shyni, T S. (2014). Analysis of Hybrid Intrusion Detection System Based on Data Mining Techniques, *International Journal of Engineering Trends and Technology* (IJETT), 15(9)p. 447-452.

[5] Weiming, Hu., Jun Gao., Yanguo Wang., Ou Wu., Stephen Maybank., Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection, (2013) *IEEE Transactions On Cybernetics*, p. 1-17.

[6] Yun Wang., Weihuang Fu., Dharma, P. Agrawal. (2013). Aussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks, (2013). *IEEE Transactions On Parallel And Distributed Systems*, 24 (2) 342-355.

7] Guisong Liu., Xiaobin Wang. (2013). An Integrated Intrusion Detection System by UsingMultiple Neural Networks, *In:* Proceedings of CIS IEEE, p 22-27.

[8] Zubair Md. Fadlullah., Hiroki Nishiyama., Nei Kato., Mostafa M. Fouda., Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks, (2013). *International Conference on Networks*, p. 51-56.

[9] Al-Jarrah, Omar., Arafat, Ahmad .(2014). Network Intrusion Detection System Using Attack Behavior Classification, *In:* Proceedings of 5th International Conference on Information and Communication Systems (ICICS) p. 1-6.

[10] Senhaji, Y., Medromi, H., Tallal, S. (2015). Network Security: Android Intrusion Attack on an Arduino Network IDS, *International Review on Computers and Software* (IRECOS), 10 (9) 950-958.

[11] Kamal Idrissi, H., Kartit, Z., Kartit, A., El Marraki, M. (2016). CKMSA: an Anomaly Detection Process Based on K-Means and Simulated Annealing Algorithms, *International Review on Computers and Software* (IRECOS), 11 (1) 42-48.

[12] Sarvari, S., Muda, Z., Ahmad, I., Barati, M., GA. (2015). SVM Algorithms for Selection of Hybrid Feature in Intrusion Detection Systems, (2015) *International Review on Computers and Software* (IRECOS), 10 (3) 265-270.

[13] Elkhadir, Z., Chougdali, K., Benattou, M. (2016). Network Intrusion Detection System Using PCA by Lp-Norm Maximization Based on Conjugate Gradient, *International Review on Computers and Software* (IRECOS), 11 (1) 64-71.

Author' s Information

Mr. M. Azhagiri has completed his Bachelor of Engineering (Information Technology) Degree from VMKV Engineering College, Salem (Vinayaka Mission's University) in the year 2009, Master of Engineering (Computer Science and Engineering) from Paavai Engineering College (Anna University) in the year 2011 and Pursuing Ph.D in Part time at St Peter's University Chennai

Dr. A. Rajesh has completed his Bachelor of Engineering (Electronics and Communication) Degree from Govt. College of Engineering, Salem (University of Madras) in the year 1997, Master of engineering (Computer Science and Engineering) from the Sathyabhama University, Chennai in the year 2005 and Completed PhD (Computer Science) at Dr.MGR University, Maduravoyil, Chennai in the year 2011.He has about 11.5 years experience in the field of education (both teaching and administration)