ISSN: 0067-2904

An Approach Based on Decision Tree and Self-Organizing Map For Intrusion Detection

Sarah M. Shareef*, Soukaena Hassan Hashim
Department of Computer Science, University of Technology, Baghdad, Iraq.

Abstract

In modern years, internet and computers were used by many nations all overhead the world in different domains. So the number of Intruders is growing day-by-day posing a critical problem in recognizing among normal and abnormal manner of users in the network. Researchers have discussed the security concerns from different perspectives. Network Intrusion detection system which essentially analyzes, predicts the network traffic and the actions of users, then these behaviors will be examined either anomaly or normal manner. This paper suggested Deep analyzing system of NIDS to construct network intrusion detection system and detecting the type of intrusions in traditional network. The performance of the proposed system was evaluated by using Kdd cup 99 dataset. The experimental results displayed that the proposed module are best suited due to their high detection rate with false alarm rate.

Keywords: Network intrusion detection system, data mining, False alarm, Decision Tree algorithm, Self-organizing map algorithm.

نظام مقترح تحليل عميق لتقليل الانذار الكاذب في نظام كشف التطفل الشبكي

سارة محمد شريف*، سكينة حسن هاشم
قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق.

الخلاصة

في السنوات الأخيرة، وقد استخدمت الإنترنت وأجهزة الكمبيوتر من قبل العديد من الناس في جميع أنحاء العالم في العديد من المجالات. وبالتالي فإن عدد المتسللين يتزايد يوما بعد يوم مما يشكل مشكلة حرجة في التمييز بين السلوك الطبيعي وغير طبيعي من المستخدمين في الشبكة. وقد ناقش الباحثون المخاوف الأمنية من وجهات نظر مختلفة. نظام كشف التسلل الشبكي الذي أساسا يحلل ، ويتنبأ حركة مرور الشبكة وسلوكيات المستخدمين، ثم سيتم فحص هذه السلوكيات إما هجوم أو سلوك طبيعي. اقترحت هذه الورقة نظام تحليل عميق لبناء شبكة نظام كشف تطفل شبكي والكشف عن نوع التطفل في الشبكة التقليدية. تم تقييم اداء النظام المقترح باستخدام kdd cup 99 . أظهرت النتائج ان النموذج المقترح هو الانسب نظرا لمعدل كشف تطفل عالي مع نسبة انذار كاذبة منخفضة.

*Email: sarahshareef84@gmail.com

1. Introduction

Nowadays, connection technology has been vastly utilized for the connecting and the transmission objective in many enforcement and large usage for security became a challenging trouble for this technology. Intrusion Detection System (IDS) are a description combination of network security [1]. IDSs are software which detects any activities that are suspected to be malicious. An IDS has two parts from an algorithmic perspective are:

Features: The evidence which recognizes abnormal activities from normal activities.

Models: The system can be put all the intrusive evidence and detect any attack [2]. Intrusion detection system implements many functions that are animated for the system. These are as follows [3]:

1- Monitoring the activities of user and system .
2- Resolving device arranging and sensibilities.
3- Appreciating system and file safety.
4- Capability for define manners representative of attack.
5- Resolve of malicious activity manners.
6- Hunting user policy wrongs.

An ID creates the huge number of alert, that decrease the efficiency of the IDS.This problem motivates many researchers to recognize alerts and reduce false positives [4]. Data Mining (DM) is usually employed within the area of intrusion detection to discovery the hidden patterns of intrusions and their relationship among each other. DM can used to learn from traffic data using supervised learning approach to detect intrusion models or unsupervised learning approach to recognize suspicious activities [5].

Feature selection was identified as an operation that selects a lower subset of features from the main set features, so that the feature area is minimized according to the evaluation criterion. Selection feature has effectiveness on intrusion detection systems performance as: it decreases the dimensionality of feature area, eliminates redundant, irrelevant, or loud data. It fetches the instant goods for implementation: speed up a DM algorithm, beneficent the quality of data, a fulfillment of data mining, and rising the understand outcomes of mining [6]. Classification is a DM mechanism which allocates subjects to one of various predefined classes. Decision tree classifier is a predictive designing method from the subfield of machine learning (ML) within the larger field of artificial intelligence. Decision trees are materials for resolving data and recognizing important features in network data which mention bad activities. DT can aid teams to define those IDS signatures to write, that firewall basics to perform and what kind of network energy to flag for more analysis [7]. There is one of the major soft computing algorithms in IDSs that Artificial Neural Network (ANN) is utilized in many discusses like detector operator. ANN was utilized to resolve a numeral of mistakes performed via other stream intrusion detection processes; The Self- Organizing Map (SOM) was a competitive network which target is to alter an input dataset of spot dimension to one or two dimensional topological plan. The Self-Organizing Map was utilized in the domains of data pressure and type estimation [8].

We will address some topics in the following sections: on section 2 we present the related work, on section 3 the KDD99 dataset is included and described, in section 4 data pre-processing of datasets is explained, in section 5 feature selection algorithm is discussed, in section 6 the proposed Deep analysing NIDS are discussed in details, section 7 evaluation performance is presented, in section 8 the experiments and results and finally the conclusion.

2. Related Work

A Survey is done consisting latest papers which execute training and testing of instrument based on decision tree and self-organizing map.

Singh R.R et al., [9], provides unsupervised learning procedures of soft computing such as (SOM) self-organizing map for detecting the intrusion detection system, neural network using legal methods of internet access to saw alarm related content at series devious web sites so this way could be useful for detecting alarms by using NSL-KDD dataset in IDS

Wu Sh.X et al., [10], added to the two-level classification framework utilizing mix of 2 data mining (DM) strategies: self-arranging guide (SOM) neural system and (K-means) clustering. First level created classification to legitimately correlate alarms identified with specific efficiency and the second characterizes alarms into categories of genuine and false alerts.then analyses demonstrate that the

suggested framework successfully decreases every single noisy alert, which frequently add to more than half of false alerts produced by a normal IDS.

Lee Joong-Hee et al., [11], instigated decision tree method for detection of intrusion. The data mining methods in intrusion detection systems (IDSs) are beneficial to notice the anomaly particularly in irregularity detection. Intended of the decision tree, will employ the DARPA98 Lincoln Laboratory assessment Data Set as the training dataset and the testing dataset. The KDD99 Intrusion Detection dataset is also depending on the DARPA set. These 3 units are comprehensively utilized in IDSs. Consequently, they demonstrated the total operation to engender the decision tree educated from the DARPA Sets. In this paper else guesstimate the efficient amount of the decision tree like the data mining manner for the IDSs and the DARPA set as the reading dataset of the decision tree.

Denatious D.K. and John A., [12]**,** characterize different data mining mechanism utilized for detecting intrusions. Again characterize the classification of Intrusion detection system and its implementation. For big value of network traffics, clustering is more convenient than classification in the area of intrusion detection because massive value of data needed to gather for utilize classification.

Aggarwal P. and Sharma S.K., [13], assess ten classification algorithms like Random Forest, Naïve Bayes C4.5, and Decision Table. They compared these classification algorithms in WEKA with KDD99 dataset. These ten classifiers were resolved according to metrics like accuracy, precision, and F-score. Random Tree displays the best outcomes aggregate in contrast the algorithms which have high detection and low false alarm rate were C4.5 and Random Forest.

3. Dataset Description

KDDCUP99 datasets has been most vastly utilized in attacks on network. This dataset is designed by Stolfo et. al. (Salvatore J. S., 2000) and is constructed depend on the data held in DARPA'98 IDS evaluation platform. The KDD training dataset include 10% of premier dataset which was approximately (494,020) single connection vectors every of which includes 41 features and was classified as either normal or an attack, with exactly one specific attack type. The training dataset has 19.69% normal and 80.31% attack connections. KDD99 is indeed consisted of three datasets. The greatest one is named (Total KDD99) this is the original dataset; the second one a subset including 10% of training data, accepted randomly from the premier dataset was generated. This (10% KDD99) dataset utilized to train the IDS, In addition to the (10% KDD99) and (Total KDD99), also is a testing dataset recognized like (Corrected KDD99) includes (14) kinds of attacks, otherwise in the whole dataset (Total KDD99) and in the training dataset (22) kinds of attacks in overall these display in Table-1, Table-2. :

Table 1- Number of model kddcup99 Datasets

Dataset of KDD	Total	Dos	R2L	U2R	Probe	Normal
Total KDD	4.898.430	3.883.370	1.126	52	41.102	972.780
Corrected KDD	311.029	229.853	16.347	70	4.166	60.593
10% KDD	494.020	391.458	1.126	52	4.107	97.277

Table 2-10% Kddcup99 of traning and testing dataset

Dataset class	Dos	U2R	R2L	Probe	Total Attack	Total Normal
Training data	79.24%	0.01%	0.23%	0.83%	80.31%	19.69%
Testing data	73.90%	0.07%	5.20%	1.34%	81.51%	19.49%

Attack type is classified into four main categories:

- **Denial of Service**: it mentions to the division that intruder prepares several computing resources too occupied to manage legal demand, or refuse legal User's incoming to instrument. DOS includes attacks: "Neptune", "back", "Apache2", "Udpstorm", "Process-table", and "teardrop".

- **Users to Root**: it mentions to the intruder begins out with incoming to natural user count on the device and was capable to deed several sensibility to gain origin access to the device. U2R includes attacks: "Spy", "Xterm", "Ps" and "Worm".
- **Remote to Local**: it indicates to the attacker transforms packets to device through a network but who does not have an count on that device and deeds some sensibility to obtain native access like an employer of that device. R2L includes attacks: "warezclient", "Named", "Xlock", "imap", "Xsnoop ", "Send-mail" and "phf".
- **Probing Attack**: it indicates to the intruder try for collect about network of systems for an evident objective for embrace its security. The PROBE includes attacks: "Ip-sweep", "satan", "Saint", and "Mscan".

4. Dataset Preprocessing

Dataset features were minimized from every of network packets, which may be irrelevant with bad prediction capability to the goal types, and several of the features may be redundant because to they are extremely inter-renovated with one of another features that decrease the detection rapidity and detection accuracy. The following step shows the preprocessing operation:

a. Normalization: is applied on the continuous features through use Min.Max algorithm, the normalization process improves effectiveness and implementation of the system by creating the values of feature in range [0 to 1].

$$V' = \frac{V - min_A}{max_A - min_A} \quad (1)$$

b. Discretization: the Kdd cup 99 dataset consists of discrete and continuous feature, therefore discretization is used to transform the continuous feature to discrete to grow speed and enclose effectiveness of the process.

5. Feature Selection Methods

Feature selection technique is the process of identifying the irrelevant and redundant feature and removing them as much as possible, to improve the effectiveness of the system by reducing the consuming time and selecting the best feature. The proposed system used entropy as feature selection algorithms as shown as Figure- 1.

Algorithm (1) shows the entropy of feature selection Input: 41 features of training dataset Output: Best five feature of training dataset
Begin Step: For all feature in training set For all value in feature 1- Calculate the probability of each value in the feature. 2- for each value in the feature calculate the entropy as Eq.2 based on probability that extracted in step 1 3- Select the best five features with the lowest value of entropy. End

Figure 1-the entropy of feature selection

6. The proposed system

The proposed deep analysing of NIDS concludes of two phases; in the first phase the proposed system training with Decision Tree (DT) algorithm thus building ID3 classifier and applying it on the Kdd cup 99 dataset to classify the type of attacks from the normal behaviour in traditional network. The proposal used 4000 records for training phase and 2000 normal in dataset.

In the second phase the proposed system training with Self Organizing Map (SOM) algorithm. SOM clustering algorithm is partition the data to various clusters according to the weight vector with

minimum Value. The proposed illustrate in Algorithm 1 shows the proposed Deep analysing system of NIDS. The two phases of proposed system is explained as follows:

Phase1: ID3 classifier used to classify the type of attacks. The result is five classes normal and four main categories of attack (DOS, Probe, U2R, and R2L).

Phase 2: SOM clustering algorithm used to cluster the type of attack into their children (subclass of type attack)

6.1 phase 1: Decision Tree (DT)

A decision tree is supervised learning procedures utilized for data discussion. DT can be represented as If-then-else rules; one of the most popular DT algorithms is ID3 which utilized shannon's entropy (ent) like a criterion for choosing the extreme significant feature as shown in equation (2.5):

$$\boldsymbol{Entropy}(\boldsymbol{s}) = \sum_{\boldsymbol{i=1}}^{\boldsymbol{c}} - \ \boldsymbol{pi}\, \boldsymbol{Log_2}\ \boldsymbol{pi} \quad (2)$$

Where: pi is rate of the types pertinence to i th category.

The suspicion in every node was minimized by selecting the attribute that most decreases its entropy. For realize this outcome; Information gain (Info gain) that degrees predictable reduction wihin entropy occasion by learning amount of a feature F_j, as shown in equation (2.6):

$$\boldsymbol{info\ gain}(\boldsymbol{S}, \boldsymbol{Fj}) = \boldsymbol{Entropy}(\boldsymbol{s}) - \sum_{\mathbf{Vi} \in \boldsymbol{V_{Fj}}} \frac{|\boldsymbol{S_{vi}}|}{|\boldsymbol{S}|} . \boldsymbol{Entropy}(\boldsymbol{S_{vi}}) \quad (3)$$

Where:

(V_{Fj}) was represented of whole potential amounts of feature (Fj)and (S_{vi}) is subset of (S) for which feature (Fj) has value (Vi).

6.2 phase 2: Self-Organizing Map (SOM) algorithm

SOM is a neural network, an unsupervised, competitive learning and clustering network that was analyzed the high dimensional data onto a set of unit's setup installed in the two or one dimensional lattice. Through a self-organizing operation, the cluster unit whose weight vector matches the input type most closely (square of minimum Euclidean distance) is selection as the gainer. The winning unit and its neighboring units update their weights as shown in equation (2.7):

$$\boldsymbol{D(j)} = \sum_{\boldsymbol{i}} (\boldsymbol{Xi} - \boldsymbol{Wij})^2 \quad \text{Euclidean distance} \quad (4)$$

Where:

D (j) is distance node with minimum unit.

Xi is the input vector.

Wij is the weight vector

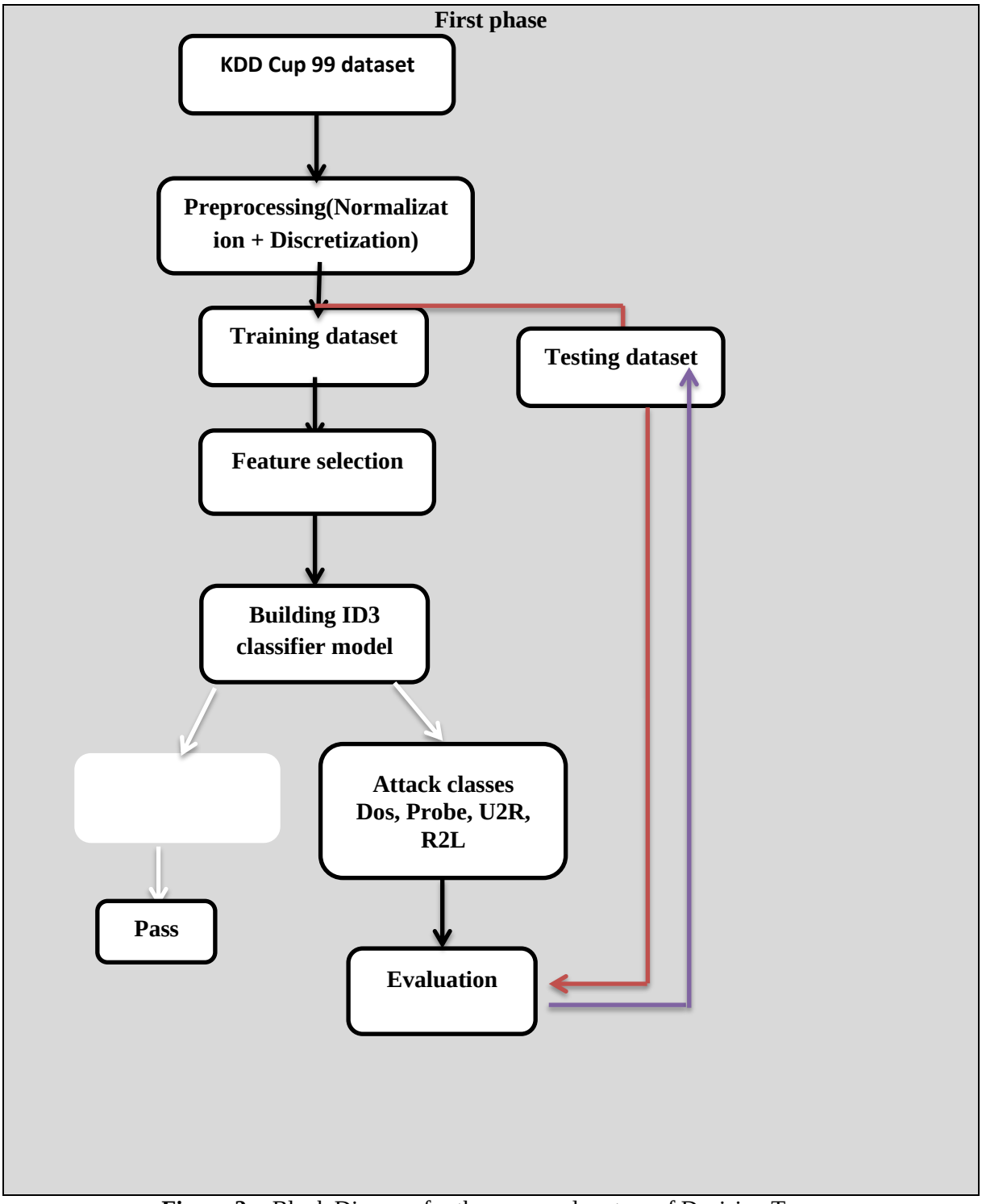

Figure 2a- Block Diagram for the proposed system of Decision Tree.

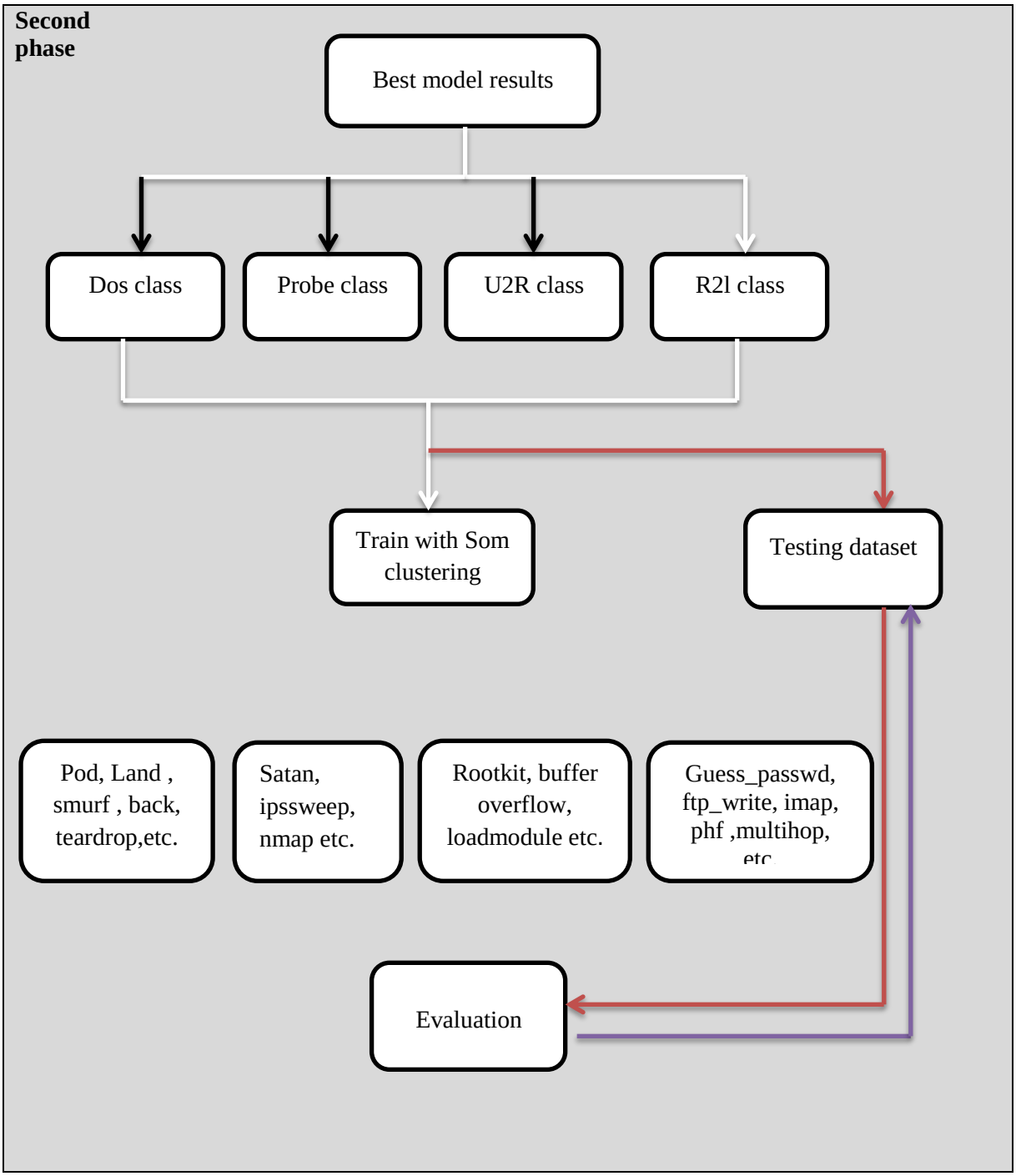

Figure 2b- Block Diagram for the proposed system of SOM

Figure 3- Deep analyzing system of NIDS

Algorithm (2) deep analyzing of NIDS
Input: Training Dataset (10% Kdd cup 99)
Output: classify the dataset into five class and clustering the type of attack into their subclass

Begin
Steps:
1- Apply Discretization preprocessing to convert continuous feature into discrete one.
2- Apply entropy feature selection and select the best five features.

//The first level of the proposed system:
1- For every class c in dataset training
- Calculate the p(c) from training dataset
- Compute the entropy of all training dataset utilizing Eq.2

End for

2- For every feature F in dataset training using Eq.2
- Compute the entropy

$$\boldsymbol{Entropy}(\boldsymbol{s}) = \sum_{\boldsymbol{i=1}}^{\boldsymbol{c}} - \boldsymbol{pi}\,\boldsymbol{Log_2}\ \boldsymbol{pi}$$

- Compute the Info gain using Eq.3

$$\boldsymbol{info\ gain}(\boldsymbol{S},\boldsymbol{Fj}) = \boldsymbol{Entropy}(\boldsymbol{s}) - \sum_{\mathbf{Vi}\in\boldsymbol{V_{Fj}}} \frac{|\boldsymbol{S_{vi}}|}{|\boldsymbol{S}|}\,.\boldsymbol{Entropy}(\boldsymbol{S_{vi}})$$

- Find the highest info gain

Repeat until all entry values are empty.
End for

//The second level of the proposed system:
1- Choose outcome layer network topology
2- Starting current neighborhood space. D(0), to a positive amount
3- Starting weights from inputs to outputs to tiny random numbers
4- Set topological neighborhood parameters
5- Set learning rate parameters.
6- Let t = 1
7- Choose an input pattern.
8- Calculate square of (Euclidean distance) from weight vectors related for every outcome node (t)
7- Choose outcome node(*j**)that has weight vector with lower Value from step: 2.
8- Update weights of whole nodes in a topological space offered by
D (*t*)*.
9- Increment *t*.
End.

7. Evaluation Measures

The measure efficiency of IDS relies on its ability to make the right detection depending on the nature of the given status compared with the outcome of intrusion detection system (IDS).The four outcomes are:

1. True negative (TN): which indicates the correct prediction of normal behaviour.
2. True positive (TP): which indicates the correct predication of attack behaviour.
3. False positive (FP) which indicate the wrong predication of normal behaviour as attack.

4. False negative (FN) which indicate mistaken predication of attack behaviour as normal. Both (TN) and (TP) are considered proof of the correct operation of the IDS. To correct the performance of the suggested system four possible results can be obtained and called confusion matrix described in Table-3.

Table (3): the confusion matrix

current category	Predicted category	
	(normal)	(attack)
1- normal	True negative(TN)	False positive(FP)
2- attack	False negative(FN)	True positive(TP)

Each of (FP), (FN) reduces the effectiveness of IDS. Therefore (FP), (FN) should be minimizing to increase the efficiency of IDS system. The performance of the proposed system evaluated using the following measures:

Accuracy (ACC): It measures performance explaining the rate of samples which are properly detected as normal or attack to the overall number of samples and calculated using the equation:

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

Detection Rate (DR): It measures performance which indicates the ratio of the number of samples that are correctly classified as attack to the total number of attack samples and is calculated using equation:

$$DR = \frac{TP}{TP+FN} \quad (6)$$

False alarm rate (FAR): It measures performance which explained the rate of samples which are improperly categorized as attack to the overall number of samples of normal behaviour and is calculated using equation:

$$FAR = \frac{FP}{TN+FP} \quad (7)$$

8. Experimental results

The proposed system evaluated with KDD99 dataset. The proposed system is trained with samples selected from KDD 99 dataset includes normal behaviour samples besides the other four types of attack (Dos, Probe, U2R, R2l) to classify the type of attack class and clustering them into their subclasses. In the Deep analysing system three evaluation criteria used to assess the proposed system which is (ACC, DR, FAR),. To check the efficiency of the proposed module two experiments are conducted, in the first experiments the algorithm is tested with dataset called dataset1 consist of (1500) records contain normal behaviour in addition to four attack types. The second experiments are conducted with datasets set called dataset2 consist of (500) records and they also include four types of attack. The result of the first level showed in Table- 4 and see Figure-1 of the decision tree , while the results of second level shown in Table- 5.

Table 4- the result of the first level of Deep analyzing system

Class type	TP rate	Fp rate	Precision	Recall	F-Measure	Dataset type
normal	1.000 1.000	0.001 0.049	0.995 0.967	1.000 1.000	0.997 0.983	Dataset 1 Dataset 2
portsweep	1.000 0.000	0.000 0.000	1.000 0.000	1.000 0.000	1.000 0.000	Dataset 1 Dataset 2
rootkit	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
neptune	1.000	0.000	1.000	1.000	1.000	Dataset 1

	1.000	0.000	1.000	1.000	1.000	Dataset 2
teardrop	0.000 0.000	0.000 0.000	0.000 1.000	0.000 1.000	0.000 1.000	Dataset 1 Dataset 2
phf	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
Spy	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
ipsweep	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
perl	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
Warezclient	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
Pod	1.000 1.000	0.000 0.000	1.000 1.000	1.000 1.000	1.000 1.000	Dataset 1 Dataset 2
land	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
satan	0.000 0.000	0.000 0.000	0.000 1.000	0.000 1.000	0.000 1.000	Dataset 1 Dataset 2
back	0.000 0.952	0.000 0.000	0.000 1.000	0.000 0.952	0.000 0.976	Dataset 1 Dataset 2
Guess_passwd	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
ftp_write	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
Buffer_overflow	0.000 1.000	0.000 0.000	0.000 1.000	0.000 1.000	0.000 1.000	Dataset 1 Dataset 2
nmap	0.000 0.000	0.000 0.000	0.000 1.000	0.000 0.909	0.000 0.952	Dataset 1 Dataset 2
Multihop	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
Load_module	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
Smurf	1.000 1.000	0.000 0.003	1.000 0.000	1.000 1.000	1.000 0.996	Dataset 1 Dataset 2

Imap	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2
Loadmodule	0.000 1.000	0.000 0.000	0.000 1.000	0.000 1.000	0.000 1.000	Dataset 1 Dataset 2
warezmaster	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	Dataset 1 Dataset 2

Table 5-the result of the second level of Deep analyzing system

Clusters	Classes rate	Dataset Type
0	1785 (89%) 19 (4%)	Dataset 1 Dataset 2
1	20 (1%) 18 (4%)	Dataset 1 Dataset 2
2	12 (1%) 45 (9%)	Dataset 1 Dataset 2
3	31 (2%) 14 (3%)	Dataset 1 Dataset 2
4	18 (1%) 21(4%)	Dataset 1 Dataset 2
5	21 (1%) 15 (3%)	Dataset 1 Dataset 2
6	8 (0%) 19 (4%)	Dataset 1 Dataset 2
7	6 (0%) 61 (12%)	Dataset 1 Dataset 2
8	8 (0%) 25 (5%)	Dataset 1 Dataset 2
9	6 (0%) 4 (1%)	Dataset 1 Dataset 2
10	8 (0%) 8 (2%)	Dataset 1 Dataset 2
11	4 (0%) 110 (22%)	Dataset 1 Dataset 2
12	12 (1%) 19 (4%)	Dataset 1 Dataset 2
13	5 (0%)	Dataset 1

	11 (2%)	Dataset 2
14	12 (1%) 2 (0%)	Dataset 1 Dataset 2
15	3 (0%) 20 (4%)	Dataset 1 Dataset 2
16	9 (0%) 10 (2%)	Dataset 1 Dataset 2
17	4 (0%) 12 (2%)	Dataset 1 Dataset 2
18	2 (0%) 19 (4%)	Dataset 1 Dataset 2
19	3 (0%) 2 (0%)	Dataset 1 Dataset 2
20	6 (0%) 30 (6%)	Dataset 1 Dataset 2
21	15(1%) 9 (2%)	Dataset 1 Dataset 2
22	2 (0%) 7 (1%)	Dataset 1 Dataset 2

9. Conclusion

In this work Deep analysing system proposed to classify the type of intrusion and clustering them into their subclasses of intrusion. The proposed work in the first level can classify the class of attack with high detection average (99%) and little false positive average (0, 05%) with dataset 1, also the detection rate (97.8%) and false positive (2.2%) with dataset 2. In the second level can detect the subclass of attack for their classes with suitable rates.

References

1. Vaidya, h., Mirza, SH. and Mail, N. **2016**. Intrusion detection System. *International Journal of advance research in engineering, science and technology*, **3**(3).
2. Mukund, Y.R., Nayak S.S and Chandrasekaran, K. **2016**. Improving False Alarm Rate in Intrusion Detection Systems using Hadoop. Inti. Conference on advance in Computing, communications and Informatics (ICACCI), India.21-24.
3. Ranga, S. and Jangra A. **2016**. A Study of IDS Technique Using Data Mining. *International Journal of Technical Research and Science*, **1**(6).
4. Gupta, N., Srivastava K. and Sharma A. **2016**. Reducing False Positive in Intrusion Detection System. (IJCSIT) *International Journal of Computer Science and Information Technologies*, 1600-1603, **7**(3).
5. Dult, I. and Dr.Borah S. **2015**. Some Studies in The Intrusion Detection Using Data Mining Techniques. *International Journal of Innovative Research in Science, Engineering and Technology*, **4**(7).
6. Bloedorn, E., Christiansen, A.D. and Hill W., Skorupka, C. and Talbot, L.M. **2001**. Data mining for Network Intrusion Detection: How to Get Started. Technical report, MITRE.

7. Novakovic, J., Strbac P. and Bulatovic, D. **2011**. Toward Optimal Feature Selection Using Ranking Methods and Classifications Algorithms. *Yugoslav Journal of operations research*, Doi: 10.2298/YJoR1119N, **1**: 119-135.
8. Atlasis, A. and Markey, J. **2011**. Using Decision Tree Analysis for Intrusion Detection: AHow-To Guide", this paper from SANS institute reading room site.
9. Singh, R.R., Gupta N. and Kumar S. **2011**. To reduce the False Alarm in Intrusion Detection System using Self Organizing Map. (IJSCE) *International Journal of Soft Computing and Engineering*,**1**(2).
10. Wu, Sh. X. and Banzhaf W. **2010**. The use of computational intelligence in intrusion detection systems:Areview. Elsevier, *applied soft computing journal*, **10**.
11. Lee, Joong-Hee, Lee Jong-Hyouk, Sohn Seon-Gyoung, Ryu Jong-Ho and Chung Tai-Myoung. **2008**. Effective value of decision tree with Kdd 99 intrusion detection datasets for intrusion detection system. Advanced communication technology, 2008, ICACT 2008. 10th international conference on feb., print ISSN:1738-9445, DOI:10.1109/ICACT.2008.4493974.
12. Denatious, D.K. and John, A. **2012**. Survey on data mining techniques to enhance intrusion detection. International conference on computer communication and informatics(ICCCI).
13. Aggarwal, P. and Sharma, S.K. **2015**. An empirical comparison of classifiers to analyze intrusion detection. Advanced computing & communication technologies (ACCT), fifth International conference on feb 2015, eISSN:2327-0659, DOI:10.1109/ACCT.2015.59.