

# Two-tier network anomaly detection model: a machine learning approach

Hamed Haddad Pajouh<sup>1</sup> ·  
GholamHossein Dastghaibfard<sup>1</sup> · Sattar Hashemi<sup>1</sup>

Received: 10 January 2015 / Revised: 2 July 2015 / Accepted: 27 October 2015 /  
Published online: 19 November 2015  
© Springer Science+Business Media New York 2015

**Abstract** Network anomaly detection is one of the most challenging fields in cyber security. Most of the proposed techniques have high computation complexity or based on heuristic approaches. This paper proposes a novel two-tier classification models based on machine learning approaches Naïve Bayes, certainty factor voting version of KNN classifiers and also Linear Discriminant Analysis for dimension reduction. Experimental results show a desirable and promising gain in detection rate and false alarm compared with other existing models. The model also trained by two generated balance training sets using SMOTE method to evaluate the chosen similarity measure for dealing with imbalanced network anomaly data sets. The two-tier model provides low computation time due to optimal dimension reduction and feature selection, as well as good detection rate against rare and complex attack types which are so dangerous because of their close similarity to normal behaviors like User to Root and Remote to Local. All evaluation processes experimented by NSL-KDD data set.

**Keywords** Anomaly detection · Intrusion detection system · Multi-layer classification · Certainty-factor

---

✉ Hamed Haddad Pajouh  
hamedhpajouh@gmail.com

GholamHossein Dastghaibfard  
dstghaib@shirazu.ac.ir

Sattar Hashemi  
s\_hashemi@shirazu.ac.ir

<sup>1</sup> Computer Science and Engineering Department, Electrical and Computer Engineering School, Shiraz University, Campus No. 2, Mollasadra Street, Shiraz 71348-51154, Iran

## 1 Introduction

Today a wide range use of network-based services and applications in almost public and private organizations require good and adoptive security measures against network and computer intrusions. Intrusions or attacks on computers and networks are activities or attempts to jeopardize main system security objectives which called as confidentiality, integrity and availability. An intrusion detection system (IDS) monitors events occurring in a computer system or a network an analysis them for sign of intrusions (Kent and Mell 2006). Network-based intrusion detection systems are generally rule-based or anomaly based. Rule-based (misuse-based) detection systems try to detect previously known patterns. The main flaw of the rule-based IDS is their weakness to detect novel attacks. But the anomaly-based approach builds a model based on behavior of normal systems after capturing network traffic and tries to detect patterns that deviate from normal behavior, which called anomaly activities, and alerts the user from these activities. Main superiority of this approach is its functionality against novel and unseen malicious activities. Anomaly detection fall into two different categories (Dua and Du 2011): supervised and unsupervised. In the supervised anomaly detection methods the normal behavior model of system or networks is established by training with a labeled dataset. These behavior models used to classify new network connection and distinguish malign or anomaly behaviors from normal ones. Unsupervised anomaly detection approaches work without any labeled training data and most of them detect malign activities by clustering or outliers-detections techniques. Based on benchmark datasets such as KDD99 and its refined version NSL-KDD which described specifically in Section 4.1, malicious activities (attacks) in network-based systems are divided into four categories:

**DoS:** Denial of Services, an attacker tries to prevent legitimate users from using service. (e.g. SYN flood),

**Probe:** an attacker tries to gain information about target host like ports scanning,

**R2L:** Remote to Local, attackers try to gain access remotely to victim machine like brute force password guessing,

**U2R:** User to Root, an attacker has local access to the target machine and tries to gain super user privilege like privilege escalation.

Most of proposed techniques are tried to gain overall detection rate (Classification Accuracy) without considering the importance of the attacks. As it is defined U2R and R2L attacks can be dangerous in comparison to the other types because they are relatively rare in the field to sample and analysis and also can causes serious damages. Although many models and methods introduced for dealing with anomalous behavior had introduced by researchers, most of them are suffer from addressing dangerous and rare attacks which belong to R2L and U2R categories. For stance Li et al. proposed an intrusion detection system based on support vector machines in Li et al. (2012) which has good detection rate against frequent attacks in training and test set like DoS and also normal behavior but its efficiency against U2R and R2L attack not very desirable. In this paper a novel supervised two-tier classification model is proposed which uses Naïve Bayes, a customized version of k-nearest neighbor (KNN) classifiers and as well as a supervised dimension reduction module to detect anomalies. The main contribution of this work against other existing methods can defined as follow:

1. Multi attack detection by using two classifiers.
2. Lower computational complexity due to optimal dimension reduction.

3. Higher detection rate against rare and dangerous attack types like U2R and R2L categories by applying Certainty-Factor (CF) for similarity measure.

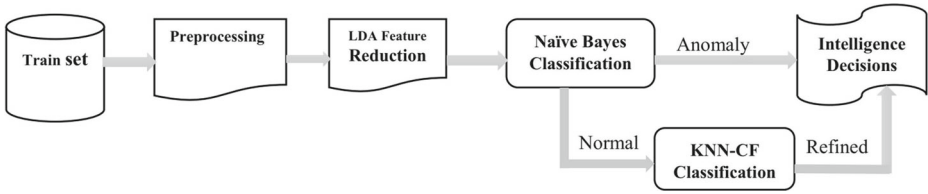
NSL-KDD (Tavallaee et al. 2009) dataset is used to evaluate the proposed model. The experimental results show a desirable detection rate against rare and complex attacks such as U2R and R2L categories. This paper is organized as follows: Related work is given in Section 2, Section 3 covers the proposed model, Section 4 gives detailed of the experiment as well as result and Section 5 covers conclusion and future research issues.

## 2 Related work

Many models have been proposed for anomaly detection based on artificial intelligence concepts. Most of the proposed models for detecting anomalous activities use statistical approaches such as cluster analysis, Bayes theory and dimension reduction (e.g. Principal Component Analysis (PCA) and fuzzy induction). Leung and Leckie (2005) for finding anomaly activities proposed an unsupervised anomaly detection model which uses density based and grid-base clustering based on subspace algorithm. They did not mention how to deal with specific attack types. Chan et al. (2005) proposed a model based on distance and density of clusters to find out that attacks were often in outlying clusters with statistically low or high densities. Zhang and Zulkernine (2006) proposed a model which combines misuse detection and anomaly detection components using the random forests algorithm, they also used high sampling by random forest to reduce dependency to previous knowledge. Toosi and Kahani (2007) combined a neuro-fuzzy network, the fuzzy inference approach and genetic algorithms to design an intrusion detection system. Their model obtained high detection rate on major attacks but still suffers from low detection rate on rare attacks. Lu and Xu (2009) proposed a three level supervised classification model using decision and Naïve Bayes and also Bayesian clustering to detect anomaly. Since their model exploit multi-level classification approach, it gains good results on different type of attacks. Panda et al. (2010) employed PCA for dimension reduction and also Naïve Bayes for classify anomalous behaviors. They applied several combination feature set to obtained result, their evaluation did not consist unseen attacks. Horng et al. (2011) proposed a model based on support vector machines (SVM) and also using BRICH (Zhang et al. 1996) clustering algorithm to extract prominent features from dataset. Their model also has high detection rate on normal and DoS classes because of their frequent pattern in both training and test set. Kromer et al. (2011) proposed a model which uses fuzzy classification and Evolutionary Algorithms for evolving fuzzy classifiers to detect anomalous activities. Kim and Kim (2014) proposed logistic regression-based anomaly detection system which exploited hierarchical feature reduction to distinguish anomalous behaviors from normal ones. Although this model proposed to address increasing detection rate of rare and dangerous attacks (U2R and R2L), increasing false alarm rate is one of its disadvantages.

## 3 Proposed model and methodology

To overcome the deficiencies in previous works, a two-tier classification model is proposed (Fig. 1). First tier consists data preprocessing and dimension reduction which has better result for decision making and first stage of classification using Naïve Bayes. At the second tier of the proposed model for better separation between normal and anomalous activities,



**Fig. 1** Two-tier classification schema which defined in the proposed model overview

specific classification using KNN-CF will be performed. A detailed explanation of the proposed model will be explained at the following sections.

### 3.1 Dimension reduction

For reducing computation time complexity and better classification multi-class Linear Discriminant analysis (LDA) will be performed (Li et al. 2006). LDA is one of the dimension reduction techniques that introduced in Izenman (2008) and it is widely used in signal processing, image processing, bankruptcy and market analysis problems. Although Principal Component Analysis (PCA) can extract features that are the most efficient for representation, it is not useful for discrimination. LDA selects an optimal projection matrix to transform a higher dimensional feature domain to a lower dimensional space while preserving the significant information for data classification (Tan et al. 2010). In the LDA technique two scatter matrices should be define, the first one is  $S_B$  which defines as between-class scatter matrix and the second one is  $S_W$  which defines as within-class scatter matrix. In the proposed model LDA scatters dataset from high dimension to lower dimension. Assume there is a set of  $n$   $d$ -dimensional samples  $x_1, \dots, x_n$  are assigned to  $k$  different classes. Each class  $C_i$ , where  $i = 1, 2, 3, \dots, k$  has  $n_i$  instances (in the proposed model  $k = 5$  e.g. normal, DoS, Probe, U2R, L2R). Projection matrix  $W$  is computed to maximize the between-class scatter matrix (1) and minimize the within-class scatter matrix (2)

$$S_B = \sum_{c=1}^k (\mu_c - \bar{x})(\mu_c - \bar{x})^T \tag{1}$$

$$S_W = \sum_{c=1}^k \sum_{i=1}^{n_c} (x_i - \mu_c)(x_i - \mu_c)^T \tag{2}$$

Where  $\bar{x}$  in (1) is mean of the whole data set denoted by:

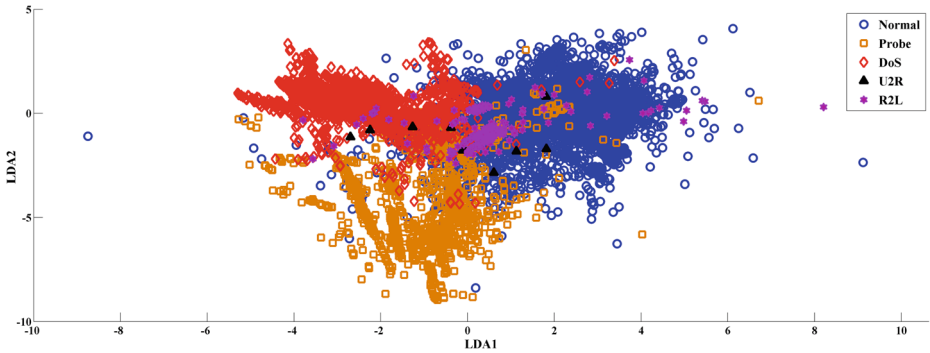
$$\bar{x} = \frac{1}{n} \sum_{j=1}^n x_j \tag{3}$$

And  $\mu_c$  is the sample mean for class  $C_i$  given by

$$\mu_c = \frac{1}{n_k} \sum_{x \in C_k} x_i \tag{4}$$

Thus, the ratio  $J$  is the between-class scatter matrix  $S_B$  and the within-class scatter matrix  $S_W$  and can be easily maximized by the projection matrix  $W_r$

$$J = \frac{W_r^T S_B W_r}{W_r^T S_W W_r} \tag{5}$$



**Fig. 2** Two dimension of train\_20 % dataset in new mapped feature space

After solving the optimization problem, we can easily perform classification on low dimension feature space by projecting the original feature space onto the optimal projection matrix  $W_r$ . The new obtained feature space has four dimensions called  $\{lda_1, \dots, lda_4\}$ . Figure 2 depicts two first dimension of mapped feature space which have optimum separation in class label instances. As it can see overlaps between classes of attack are still exist and they should be addressed.

### 3.2 Naïve Bayes classifier

Naïve Bayes is an efficient and effective classification algorithm since it assumes all attributes of each instance are independent in given class (conditional independence assumption). Despite the fact that assumption are violated in most of the time, the generated result are so promising and desirable.

In Naïve Bayes, an instance (object) is defined by a feature vector with  $n$  attributes,  $X = (x_1, x_2, \dots, x_n)$ . Suppose there are  $m$  class labels  $C_1, C_2, \dots, C_m$ , next calculate  $P(C_i|X)$  for  $(k = 1, 2, \dots, m)$  and select the maximum of  $P(C_i|X)$ . Then, the object  $X$  is classified into category  $C_i$ , where  $P(C_i|X)$  is posterior probability and defined by:

$$P(C_i|X) = \frac{P(C_i|X)P(X)}{P(X)} \tag{6}$$

Since  $P(X)$  is a constant, in the proposed model only  $P(C_i|X)P(C_i)$  will be calculated and then the maximum value will be selected. Since in Naïve Bayes, attributes are independent, therefore it uses (7) for computing probability multiplication:

$$P(C_i|X) = \prod_{k=1}^n P(X_k|C_i) \tag{7}$$

**Table 1** Assessment of new mapped attributes dependency by correlation coefficient measure in Train\_20 %

Features	$lda_1$	$lda_2$	$lda_3$	$lda_4$
$lda_1$	1	0	0	0
$lda_2$	0	1	0	0
$lda_3$	0	0	1	0
$lda_4$	0	0	0	1



**Table 4** Classification of attacks in NSL-KDD data set

Main class	Attacks types
DoS	back, land, neptune, pod, smurf, teardrop.
Probe	ftp write, guess passwd, imap, multihop, phf, spy, warezclient, warezmaster.
U2R	buffer overflow, perl, loadmodule, rootkit.
R2L	ipsweep, nmap, portsweep, satan.

problem. To address this issue, certainty factor (CF) associated with Euclidean distance is adopted for similarity measure in the new feature space (Zhang 2010).

CF measures incorporated in KNN classification are as follows.

- Let  $N(Q, k)$  be  $k$  nearest neighbor of  $Q$
- $p(C = c_i|D)$  be the ratio of  $c_i$  in training set  $D$
- $p(C = c_i|N(Q, k))$  be the ratio of  $c_i$  in the query result.

Now  $CF$  can be computed using (8) and (9) as follows:

if  $(p(C = c_i|N(Q, k)) \geq p(C = c_i|D))$

$$CF(C = c_i, N(Q, k)) = \frac{(p(C = c_i|N(Q, k)) - p(C = c_i|D))}{(1 - p(C = c_i|D))} \tag{8}$$

else

$$CF(C = c_i, N(Q, k)) = \frac{(p(C = c_i|N(Q, k)) - p(C = c_i|D))}{(p(C = c_i|D))} \tag{9}$$

Values of  $CF(C = c_i, N(Q, k))$  are in the range of  $[-1, 1]$ . The CF strategy for KNN classification is defined as follows.

$$SCF = \operatorname{argmax} CF\{(C = c_i, N(Q, k))\} \tag{10}$$

Before performing classification, for better separation between normal and anomalous classes feature selection will be performed. As mentioned, new feature space consists of four dimensions, in this phase PCA feature selection will be used which selects two effective features ( $lda_1, lda_2$ ) out of four and then classification will be applied. To improve classifier performance in KNN classifier, a bucketing technique using KD-tree data structure is applied to store the reduced training set (Friedman et al. 1977). At this stage a detailed analysis of the proposed model will be explained. The proposed model converts a high dimension data set into lower one and performs its classification by two machine learning classifier. The experimental results will be discussed in the next section.

**Table 5** NSL-KDD data set classes distribution

Datasets	Total records	Normal	Probe	DoS	U2R	R2L
Train_20 %	25192	13449	2289	9234	11	209
Train <sup>+</sup>	125973	67343	11656	45927	52	995
Test <sup>+</sup>	22544	9711	2421	7458	67	2887

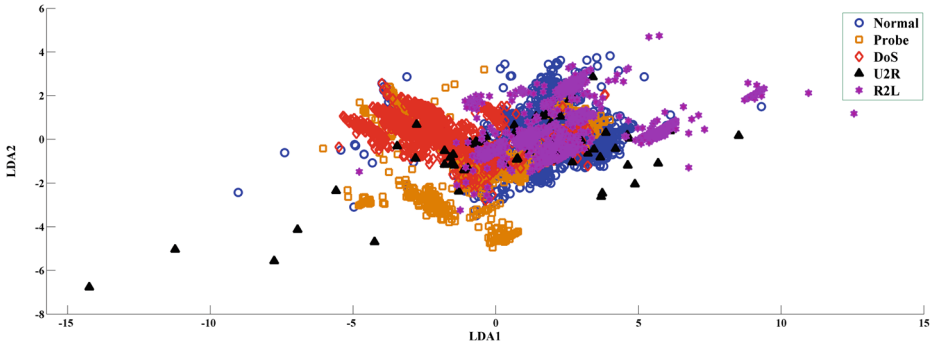


Fig. 3 Two first dimension of the test set which mapped by projection matrix of NSL-KDD training set

### 4 Evaluation and experimental result

At this section first a detailed analysis of the applied dataset will be discussed, then IDS performance metrics will be defined and finally evaluation of the proposed model will be argued.

#### 4.1 NSL-KDD dataset

To evaluate the proposed model NSL-KDD benchmark dataset is used. NSL-KDD (Tavallae et al. 2009) dataset is new version of KDD99 (KDD Cup 1999) dataset this data set introduce for network intrusion detection systems competition. Each NSL-KDD record consists of a host-to-host connection which has 41 distinguished features (e.g., protocol type, service and flag) and are labeled as normal, anomaly or one of the specific attack names as it presented in Table 4. All attacks fall into four major group: DoS, probe, U2R and R2L. The feature vector consists of three categorical values; five symbolic values and the rest of them are continuous values.

Since there were some flaws in original KDD dataset (Panda et al. 2010) and (Tavallae et al. 2009), in order to evaluate the proposed model NSL-KDD dataset applied. The dataset came with two training set and one test set which contains DoS, Probe, U2R, R2L attack classes beside normal label. Table 5 shows the distribution of class labels in both training set and test set. Test set also containing 17 attack types which did not observe in training set, according to this issue, we can evaluate the proposed model by unseen attacks to show its effectiveness. Although the dataset is refined and does not have redundancy, it still suffers from some problems (McHugh 2000).

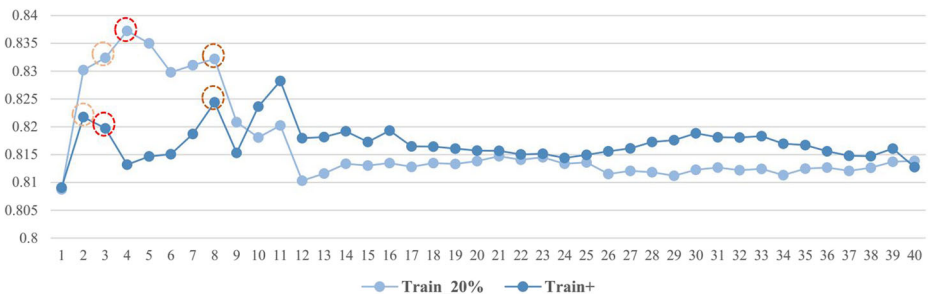


Fig. 4 Detection rate experiment over different k values by NSL-KDD data set



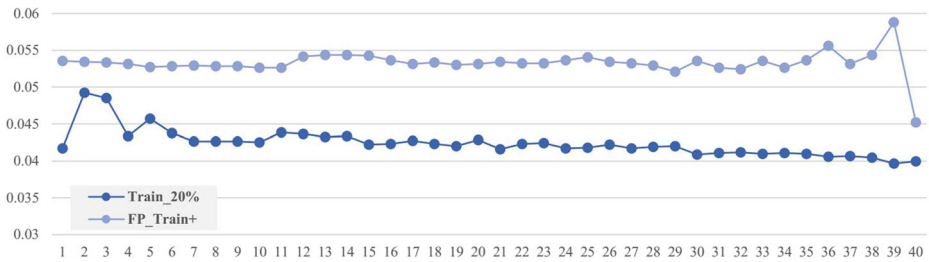


Fig. 5 False Positive rate experiment over different k values by NSL-KDD data set

### 4.2 Data preprocessing

In the data preprocessing phase for better decision making and mitigating the computational overhead, the original dataset will be converted to a normal form (Han and Kamber 2006), it will be as follows:

- Each categorical feature values will be assigned to a unique integer number like (TCP = 1, UDP = 2, ICMP = 3).
- Continuous-valued features will be discretized using logarithm to the base 2 and then casting the result value to integer for avoiding any bias. This step uses (11) for each Continuous-valued z.

$$if(z \geq 2)z = \int \log_2(z + 1) \tag{11}$$

After the normalization for better classification, attack labels will be grouped into four major classes and a normal class.

### 4.3 Performance metrics

Performance indicators (Gu et al. 2006) for the intrusion detection systems are: True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN), detection rate and false alarm rate, where:

**TP** represents that the normal behavior which is correctly predicted as normal,

**TN** represents the anomaly behavior which is detected correctly,

**FP** shows that the anomalous behavior which is predicted as normal,

**FN** means that the normal behavior which is wrongly thought as anomalous behavior,

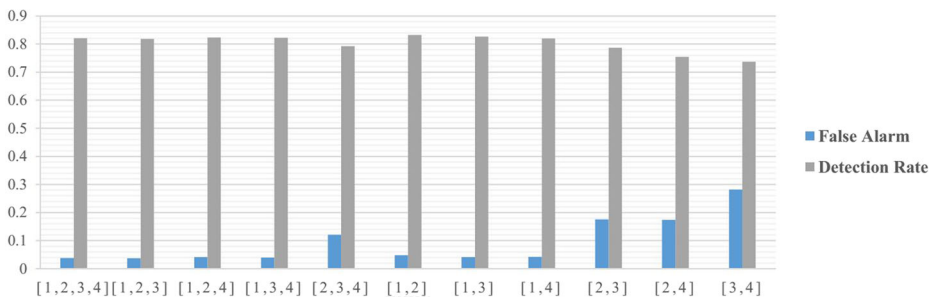


Fig. 6 Comparison between detection rates and false alarms using different new mapped feature subsets of NSL-KDD data set

**Table 6** Comparison between anomalous instances detection rates (%) of the first level and the refined level of classification

Level	Probe	DoS	U2R	R2L
First level of classification	81.24	78.81	52.23	14.99
Refined level of classification	86.12	85.29	58.21	36.06

Detection rate:  $DR = \frac{TP}{FN+TP}$

False alarm rate:  $FAR = \frac{FP}{FP+TN}$

Classification Accuracy:  $CA = \frac{TP+TN}{P+N}$

#### 4.4 Complexity analysis

As it said in the contributions section, model provided “lower computational complexity due to optimal dimension reduction”. With regard to this reduction, in the first tier Naïve Bayes classifier applied which its computational complexity is defined as  $O(e \times f)$ , where  $e$  is number of objects in dataset and  $f$  indicates number of attributes. Therefore at this stage, according to LDA transformation the classifier will be fed with only four attributes instance of 41, the computation complexity reduced by ten fold. On other hand at the second tier where KNN classifier is applied, model just needed to remember only two dimensions of training set. As a result of that it would takes up less space than indigenous dataset. In addition the bucketing technique (k-d tree) is used for searching nearest neighbors and due to the preprocessing phase, which all features have an integer value, finding nearest neighbor will be more convenient and in such (two dimensions) k-d tree points takes  $O(\log n)$  time on average.

#### 4.5 Testing environment and results

The experiment was processed within a MATLAB R2013a environment, which was running on a PC powered by AMD Phenom II X6 3.8 GHz CPU and 12 GB RAM.

The proposed model was trained by both training set ( $Train_{20\%}$ ,  $Train^+$ ) and then evaluated by given test set ( $Test^+$ ) provided by NSL-KDD which contains 22544 instances. So all the given results in this research are evaluated by this test set. After normalizing test set, the projection matrix ( $W_r$ ) which obtained from training test applied to test set. As Fig. 3 illustrates the scattering rates of mapped test set not much variant from training set. Another important issue which implies from this figure is the rare and dangerous attack like R2L are so involved with normal behaviors. But the proposed model can almost solve this issue by using k nearest neighbor as it second classifier. Figure 4 shows the result of KNN classification detection rates for various  $k$  values, at this step 40 iterations is experimented. According to detection rates of this experiment three  $k$  values nominated to applied in the proposed model,  $k = 3$  is chosen because of obtaining better detection rate on rare class of attacks in comparison with other nominated values. Figure 5 depicts effects of this experiment on false positive rate (FPR) in both given training set, these results show there is no significant

**Table 7** Multi-class classification Detection Rates (%) comparison to existing models

Method	Normal	Probe	DoS	U2R	R2L
Proposed model	94.56	79.76	84.68	67.16	34.81
HFR-MLR method (Kim and Kim 2014)	93.70	80.2	89.70	29.50	34.20

**Table 8** Confusion matrix of existing models which had low false alarm and undesirable detection rate (%) against the rare attacks versus proposed model

Model	Normal	Probe	DoS	U2R	R2L
The proposed model	94.56	79.76	84.68	67.16	34.81
SVM with BIRCH clustering (Zhang et al. 1996)	99.3	99.5	97.5	28.8	19.7
ESC-IDS (Toosi and Kahani 2007)	98.2	99.5	84.1	31.5	14.1
Association rule (Xuren et al. 2006)	99.5	96.8	74.9	0.79	0.38

changes in FPR for different  $k$  values. Figure 6 shows comparison between detection rates and false alarms on the all possible combinations of new mapped features in *Train\_20 %* training set. According to this experiment the highest detection rate belongs to combination of the two first attribute ( $lda_1, lda_2$ ). To show usefulness of the proposed model concept for using two level of classification, in Table 6 Detection rates of the first level which belongs to anomalous instances is compared to final decision on incoming objects from test set.

We also gained 4.83 % false alarm using *Train\_20 %* dataset and 5.44 % in using *Train<sup>+</sup>* as training set and using *Test<sup>+</sup>* respectively for testing the proposed model. The comparison results in Table 7 shows that the proposed model obtained better detection rate in normal and the rare attacks (U2R, R2L) and also a close detection rates to other types of attacks against one of the recent works. In comparison to the two classification models, the proposed model also obtained a desirable results.

it worth noting that this model is proposed to tackle with deficiency of other existing models in detecting the rare class attacks which is located in the data set and also gaining a promising detection rates of the other types of attack. In addition, the model must compare with multi-class classification ones like HFR-MLR (Kim and Kim 2014) which presented a solution for the same issue. As it can be seen in Table 7. The proposed model outperformed U2R attacks detection rate by two fold increase and also made progress in R2L attacks, in addition the model also caused lower false alarm comparing with one of the latest methods (Kim and Kim 2014). Moreover it should mention that in HFR-MLR authors present their results by experimenting multi-set of attributes which still shows an uncertainty for choosing right attributes set.

As a downside, the proposed model cannot provide an impressive detection rate compared with existing models which had better results confronted the routine attack types like

**Table 9** Single-layer Vs. multi-layer binary classification comparison (%) result evaluated by *Test<sup>+</sup>*

Method	Training set	detection rate	False alarm rate
Proposed model	<i>Train_20 %</i>	83.24	4.83
Naive Bayes (Tavallae et al. 2009)	<i>Train_20 %</i>	76.56	N/A
Random forest (Tavallae et al. 2009)	<i>Train_20 %</i>	80.67	N/A
SVM (Tavallae et al. 2009)	<i>Train_20 %</i>	69.52	N/A
Decision trees (J48) (Tavallae et al. 2009)	<i>Train_20 %</i>	81.05	N/A
Proposed model	<i>Train<sup>+</sup></i>	82	5.43
SOM IDS (Ibrahim et al. 2013)	<i>Train<sup>+</sup></i>	75.49	N/A
Feature selection with SVM IDS (Pervez and Md Farid 2014)	<i>Train<sup>+</sup></i>	82	15

**Table 10** Generated training set by SMOTE technique

Datasets	Total records	Normal	Probe	DoS	U2R	R2L
Train_20 %	25192	13449	2289	9234	11	209
Train_20 % 5x(R2L & U2R)	26292	13449	2289	9234	66	1254
Train_20 % 6xR2L & 16xU2R	29854	13449	2289	9234	67	2508

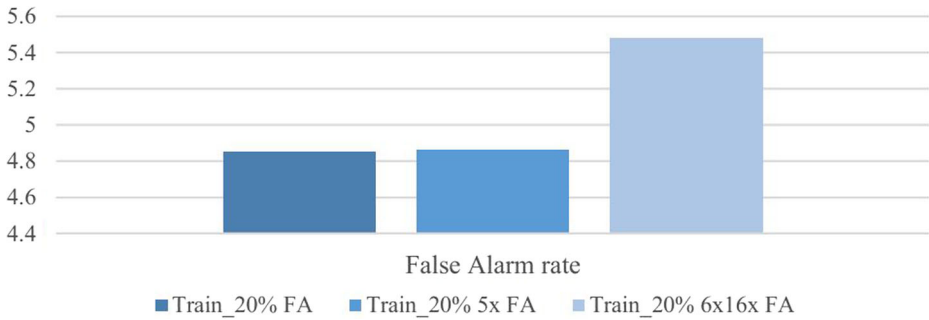
DoS and Probe. In one of the latest approaches (Pervez and Md Farid 2014) which uses SVM classifier to battle anomaly in network, average of classification accuracy is about 81.4 percent and the best obtained accuracy based on figure is about 82.68, in the meanwhile our presented approach obtained 83.24 with a distinction separation among attack types and improve detection rate in the rare ones. Further more the proposed model gained much lower false alarm rate, 5 percent against 15 percent. The undeniable issue is that, it is virtually impossible to have a significant detection rate against the rare attacks and also having impressive low false alarm. As in Table 3 mentioned In the training set we have two feature vectors with the same values but with different class labels. Thus if it is focused on the comparison of false alarm versus these types of attack it be can seen that they have distinct issues. Let's take a glance at other existing models which had impressive low false alarm and their detection rate against the rare attacks (Table 8), this discrepancy will be revealed.

In this work two-class (normal or anomaly) of anomaly detection classification problem is also considered, each arriving object which gave one of attack label called as anomaly and other named as normal behavior. Table 9 also provides a binary classification comparison between one-tier approaches and the proposed model which exploited two classifiers. As it can be seen the two-tier model outperformed the others in both detection and false alarm rates.

For evaluating the second tier similarity measure (CF) SMOTE (Chawla et al. 2011) technique was used to generate two balanced training sets from Train\_20 % dataset. In the first training set rare instances distribution which belong to U2R and R2L classes have been increased five times and in the second training set tried to make dataset balance by increasing rare attacks class label distribution. Table 10 shows original training set class labels distribution and the generated ones. For evaluating the similarity measure, the proposed model run with and without CF measure. The results show no significant improvement in detection rate of rare classes and also higher false alarm in compared with CF measure. Table 11 shows the obtained detection rate. Figure 7 depicts the proposed model false alarm rate when it used CF similarity measure with original training set and when it did not. As it can be seen CF similarity measure false alarm rate using imbalance training set (original) is lower from the generated training sets.

**Table 11** Detection Rates (%) comparison to Generated training sets using SMOTE technique

Datasets	Normal	Probe	DoS	U2R	R2L
Train_20 %	95.15	86.12	85.29	58.21	36.06
Train_20 % 5x(R2L & U2R)	95.14	86.95	85.64	65.67	17.70
Train_20 % 6xR2L & 16xU2R	94.52	90.95	86.06	55.22	39.63



**Fig. 7** comparison between false alarm rates of proposed model on different training set within and without CF similarity measure

## 5 Conclusion and future works

This paper is proposed a network anomaly detection model which used a data preprocessing, LDA feature reduction module and also two level classifier. The proposed model works with only four mapped feature out of 41 distinguished attributes of NSL-KDD Datasets. Applying two level of classification by Naïve Bayes and CF-KNN which led to gain higher detection rate on the rare and dangerous types of attacks in comparison to existing models.

In summary, if we want to weigh up the pros and cons of the proposed model on the positive side, the two-tier anomaly detection does not need to remember high dimensional and heavy training set for the model consumption due to dimension reduction by LDA and also a feature selection in the second tier and also by such reduction the computation in both tier is reduced. In addition the proposed model relatively relieve the problem of insufficient dealing with the rare attacks which have same behaviors to normal ones due to their feature vectors, which located in training set, by certainty factor similarity measure. But in other hand the model still is incapable to gain the appropriate detection rate against routine and less dangerous kind of attack yet.

For extending the proposed model, we are investigating other dimension reduction technique such as non-parametric techniques for obtaining more useful features and also we are working on fuzzy clustering techniques for better separating normal instances from the anomalous ones to increasing detection rate.

## References

- Bouzida, Y., & Cuppens, F. (2006). Neural networks vs. decision trees for intrusion detection. In *IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (MonAM), Tuebingen* (pp. 28–29).
- Chan, P.K., Mahoney, M.V., & Arshad, M.H. (2005). Learning Rules and Clusters for Anomaly Detection in Network Traffic. *Managing Cyber Threats: Issues, Approaches and Challenges*, 5, 81–99.
- Chawla, N.V., Bowyer, K.W., Hall, L.O., & Kegelmeyer, W.P. (2011). SMOTE: synthetic minority over-sampling technique, arXiv:11061813.
- Dua, S., & Du, X. (2011). *Data Mining and Machine Learning in Cybersecurity*. USA: CRC Press.
- Friedman, J.H., Bentley, J.L., & Finkel, R.A. (1977). An algorithm for finding best matches in logarithmic expected time. *ACM Transactions on Mathematical Software TOMS*, 3(3), 209–226.
- Gu, G., Fogla, P., Dagon, D., Lee, W., & Skori, B. (2006). Measuring intrusion detection capability: An information-theoretic approach. In *Proceedings of the ACM Symposium on Information, computer and communications security* (pp. 90–101).

- Han, J., & Kamber, M. (2006). *Data mining concepts and techniques*. Amsterdam; Boston; San Francisco: Elsevier; Morgan Kaufmann.
- Hornig, S.J., Su, M.Y., Chen, Y.H., Kao, T.W., Chen, R.J., Lai, J.L., & Perkasa, C.D. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. *Expert Systems with Applications*, 38(1), 306–313.
- Ibrahim, L.M., Basheer, D.T., & Mahmod, M.S. (2013). A Comparison Study for Intrusion Database (KDD99, NSL-KDD) Based on Self Organization Map (SOM) Artificial Neural Network. *Journal of Engineering, Science and Technology*, 8(1), 107–119.
- Izenman, A.J. (2008). *Modern Multivariate Statistical Techniques*, (pp. 237–280). New York: Springer.
- KDD Cup (1999). Data, <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>, Accessed 17 September 2014.
- Kent, K., & Mell, P. (2006). Guide to Intrusion Detection and Prevention (IDP) Systems, Natl. Inst. Stand. Technol., USA.
- Kim, E., & Kim, S. (2014). A Novel Anomaly Detection System Based on HFR-MLR Method. *Mobile, Ubiquitous and Intelligent Computing*, 274, 279–286.
- Kromer, P., Platos, J., Snašel, V., & Abraham, A. (2011). Fuzzy classification by evolutionary algorithms. In *IEEE International Conference on Systems, Man and Cybernetics (SMC)* (pp. 313–318).
- Leung, K., & Leckie, C. (2005). Unsupervised anomaly detection in network intrusion detection using clusters. In *Proceedings of the Twenty-eighth Australasian conference on Computer Science*, (Vol. 38 pp. 333–342).
- Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. *Expert Systems with Applications*, 39(1), 424–430.
- Li, T., Zhu, S., & Ogihara, M. (2006). Using discriminant analysis for multi-class classification: an experimental investigation. *Knowledge and Information Systems*, 10(4), 453–472.
- Lu, H., & Xu, J. (2009). Three-Level Hybrid Intrusion Detection System. In *International Conference on Information Engineering and Computer Science, ICIECS09* (pp. 1–4).
- McHugh, J. (2000). Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory. *ACM Transactions on Information and System Security*, 3(4), 262–294.
- Panda, M., Abraham, A., & Patra, M.R. (2010). Discriminative multinomial naive bayes for network intrusion detection. In *Sixth International Conference on Information Assurance and Security (IAS)* (pp. 5–10).
- Pervez, M.S., & Md Farid, D. (2014). Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs. In *8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)* (pp. 1–6).
- Tan, Z., Jamdagni, A., He, X., & Nanda, P. (2010). Network Intrusion Detection based on LDA for payload feature selection. In *GLOBECOM Workshops (GC Wkshps)* (pp. 1545–1549). Miami: IEEE.
- Tavallae, M., Bagheri, E., Lu, W., & Ghorbani, A.-A. (2009). A detailed analysis of the KDD CUP 99 data set. In *Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defense Applications*.
- Toosi, A.N., & Kahani, M. (2007). A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. *Computer and Communications*, 30(10), 2201–2212.
- Xuren, W., Famei, H., & Rongsheng, X. (2006). Modeling Intrusion Detection System by Discovering Association Rule in Rough Set Theory Framework. In *International Conference on Computational Intelligence for Modeling, Control and Automation, and International Conference on Intelligent Agents, Web Technologies and Internet Commerce* (p. 2424).
- Zhang, S. (2010). KNN-CF Approach: Incorporating Certainty Factor to kNN Classification. *IEEE Intell. Inform. Bull.*, 11(1), 24–33.
- Zhang, T., Ramakrishnan, R., & Livny, M. (1996). BIRCH: an efficient data clustering method for very large databases. In *ACM SIGMOD Record*, (Vol. 25 pp. 103–114).
- Zhang, J., & Zulkernine, M. (2006). Anomaly based network intrusion detection with unsupervised outlier detection. In *IEEE International Conference on Communications, ICC06*, (Vol. 5 pp. 2388–2393).