Intrusion Detection System using SMIFS and Multi class Multi layer Perceptron

V Maheshwar Reddy, I Ravi Prakash Reddy, K Adi Narayana Reddy

***Abstract*— As the new technologies are emerging, data is getting generated in larger volumes high dimensions. The high dimensionality of data may rise to great challenge while classification. The presence of redundant features and noisy data degrades the performance of the model. So, it is necessary to extract the relevant features from given data set. Feature extraction is an important step in many machine learning algorithms. Many researchers have been attempted to extract the features. Among these different feature extraction methods, mutual information is widely used feature selection method because of its good quality of quantifying dependency among the features in classification problems. To cope with this issue, in this paper we proposed simplified mutual information based feature selection with less computational overhead. The selected feature subset is experimented with multilayered perceptron on KDD CUP 99 data set with 2- class classification, 5-class classification and 4-class classification. The accuracy is of these models almost similar with less number of features.**

***Keywords* — IDS, Perceptron, Mutual Information, Entropy, Conditional Entropy, Feature Selection.**

1. INTRODUCTION

Intrusion detection system [3, 19, and 20] dynamically detects and monitors the activities that occur in the network and analyzes the malicious activity which violates the security policy and user security. Intrusion detection is categorized into misuse and anomaly detection. In misuse detection the incoming and outgoing packet signatures are compared against a database of signatures. Anomaly detection creates a profile for the normal behavior and any activity that deviates from the profile is considered as an attack. There is continuous growth in attacks on the network from the last three decades. The attacks are impacted lot on the user security. It is difficult to handle these attacks traditionally. To handle these attacks automatically, lot of research [1-10] is carried on intrusion detection system using machine learning. Machine learning algorithm requires the past data to train the model. The IDS using machine learning is built on the standard data sets like KDD CUP 99, NSL-KDD, Kyoto-2006+, ISCX, etc. The KDD CUP 99 data set is the most popular and standard data set used in the literature. The data is collected and distributed by MIT Lincoln laboratory and is sponsored by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory (AFRL). The KDD CUP 98 and KDD CUP 99 data sets are a subset of DARPA sponsored project. The [23] KDD CUP 99 data set contains 41 features and a class label. The class label is multi-class and it has five classes namely Normal, DOS, Probe, R2L and U2R.

Feature selection [1, 2, 6, 7, 12, 13] is an important technique in selecting the subset of important features from the high dimensional data. This technique extracts relevant features and removes the redundant features. The feature selection approaches are categorized into filter based and wrapper based techniques. The wrapper based technique is dependent on classification algorithm whereas filter based technique extracts the subset of features, independent of classification algorithm. Most of the researchers developed the IDS models using machine learning algorithms with the different feature selection technique combinations. The ranking methodology and SVM are used in [21] as feature selection and classification algorithm. Similarly GA and decision tree algorithm in [22], PCA and SVM algorithm in [4], GA and SVM algorithm in [2] and rough set theory and SVM with different kernel functions in [14] are used as feature selection and classification algorithms. The feature selections techniques like correlation based feature selection, consistency based filter and INTERACT are introduced in [3]. The naïve Bayes, tree augmented naïve Bayes and NBTree are trained on the selected subset of features. The relevant features are selected using BIRCH hierarchical clustering algorithm in [6] and in [5] bagging with REPTree is trained on these selected features. These feature selection techniques are wrapper based and works with only the specific classification algorithm. We propose a feature selection technique based on mutual information. This technique is a filter based feature selection technique. In the next section we cover the literature on mutual information based filtering technique.

The paper is organized as, section two deals with concepts of entropy, joint entropy, conditional entropy, and mutual information along literature survey on mutual information. Section 3 covers the proposed simplified mutual information based feature selection. Section 4 deals with experimental setup and results and the final section concludes the paper.

2. MUTUAL INFORMATION

Mutual Information is originally proposed by Claude E. Shannon [15, 16] in the year 1948 in his research paper “A Mathematical Theory of Communications.” Entropy and conditional entropy are the smallest units of mutual information. Mutual information measures the dependency between two variables. The entropy measures the uncertainty of a random variable. The entropy of a random

Revised Manuscript Received on July 10, 2019.

V Maheshwar Reddy, Assistant Professor ACE Engineering College, Telangana, India.

I Ravi Prakash Reddy, Professor, G. Narayanamma Institute of Technology and Science, Telangana, India.

K Adi Narayana Reddy, Professor, ACE Engineering College, Telangana, India.

Retrieval Number: I8982078919/19©BEIESP
DOI:10.35940/ijitee.I8982.078919

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

variable X, joint entropy and conditional entropy of two random variables X and Y are defined respectively as

$$H\,(X) = -\sum_{x\,\in X} p(x)\,.\log p(x) \qquad (1)$$

$$H\,(X\,,Y) = -\sum_{x\,\in X}\sum_{y\,\in Y} p(x,y)\,.\log p(x,y) \qquad (2)$$

$$H\,(Y\mid X) = -\sum_{x\,\in X}\sum_{y\,\in Y} p(x,y)\,.\log p(y|x) \qquad (3)$$

Here p(x, y) is the probability density function. The relationship is between joint entropy and conditional entropy is defined as

$$MI\,(X\,,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y) \qquad (4)$$

Where H(X, Y) and H(X/Y) / H(Y/X) are joint entropy and conditional entropy respectively. The relationship between the entropy, conditional entropy, joint entropy and mutual information is shown fig 1.

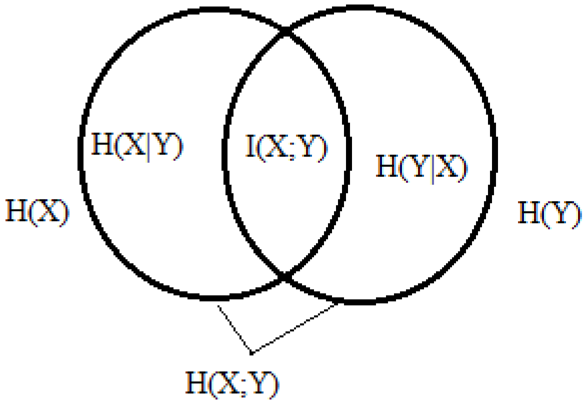

Fig 1: Relationship between entropies and mutual information

For two discrete random variables, the mutual information(MI) is defined as

$$MI\,(X,Y\,) = \sum_{x\varepsilon X}\sum_{y\varepsilon Y} P(x,y)\,.\;log\,\frac{p(x,y)}{p(x)\,.\;P(y)} \qquad (5)$$

The MI between two continuous random variables X and Y is defined as

$$MI(X\,,Y) = \int_x\int_y p(x,y).\log p(x,y)dxdy \qquad (6)$$

Here P(x), P(y) and P(x, y) are marginal density function of X, marginal density function of Y and joint probability density function of x, y respectively. The variables X and Y are dependent If MI(X, Y) is very high and independent if MI(X, Y) is zero.

Many researchers[1,2,6,9,11,12,24,25,26,27,28] used mutual information to select the sub set of features from the -feature set and built the predictive models on the subset of features to classify the attacks in IDS. Battiti [10] proposed mutual information based feature selection in which a greedy selection procedure is applied based on the equation (7). This calculates the MI between candidate feature and class label using selected features and we select the feature with highest mutual information into the feature subset. Here β lies between 0.5 and 1.

$$\max\left\{MI\,(Fi\,;\,C) - \beta\sum_{fi\in F, fs\in S} MI(fi\,;\,fs)\right\} \qquad (7)$$

The MIFS-U is a variation of MIFS and was proposed by Nojun Kwak et.al. [11] in the year 2002. The MIFS-U is defined in equation (8) as

$$\max\left\{MI\,(Fi\,;\,C) - \beta\sum_{\substack{\mathrm{fi}\in F\\ \mathrm{fs}\in S}}\frac{MI\,(C\,;fs)}{H(fs)}MI(fi\,;\,fs)\right\} \qquad (8)$$

where $H(fs)$ is the entropy of the selected feature. In 2003, D Huang et.al. [6] and in 2005, Tommy W S Chow et. al [7] proposed optimal feature subset using mutual information (OFS-MI). The OFS-MI uses Feature Relevancy Criteria (FRC) and Feature Similarity Criteria (FSC). FRC selects the relevant features using FRC (f) =MI (F, S, C) and FSC reduces the redundancy among the selected feature using the similarity between the features. A candidate feature becomes selected feature if FSC (F,S) ≥ θ, where θ value is fixed with 0.5.

$$\max\,\{\,MI\,(f\,;\,fi)\,,H(fi)\,\} \qquad (9)$$

To overcome the drawbacks of OFS-MI H. Peng et.al [9] proposed another feature selection in 2005 which is minimal redundancy and maximum relevance (mRMR). The mRMR minimizes the redundancy between the features and maximizes the dependency among the selected feature subset and class labels. It consists of two stages; in the first stage it finds the feature subset with minimum error rate and low classification error. In the second stage a greedy forward selection and backward elimination procedure is applied based on the formula (10) by replacing β with |S| in (8).

$$\max\left\{MI\,(Fi\,;\,C) - \frac{1}{|S|}\sum_{\substack{\mathrm{fi}\in F\\ \mathrm{fs}\in S}} MI(fi\,;\,fs)\right\} \qquad (10)$$

In 2008, another estimation of MIFS was proposed by Huang JJ et.al. [17] called MICC in which entropies of candidate feature and selected features also used to extract the features in forward selection procedure with the equation (11).

$$\max\left\{\frac{MI\,(C\,;\,fi)}{\frac{1}{|S|}\sum_{\substack{\mathrm{fi}\in F,\\ \mathrm{fs}\in S}}\frac{MI\,(\,fi\,;fs)}{\min\{\,E(fi),E(fs)\}}} - MI\,(fi\,;\,C)\right\} \qquad (11)$$

An enhanced version of MIFS, MIFS-U, mRMR is proposed by Pablo A. Estevez et.al. [13] in the year 2009 and is known as normalized mutual information based feature selection (NMIFS). The NMIFS uses normalized MI, in which it finds the relevant features based on the equation (12).

$$\max\left\{MI\,(Fi\,;\,C) - \frac{1}{|S|}\sum_{\substack{\mathrm{fi}\in F\\ \mathrm{fs}\in S}}\frac{MI(fi\,;\,fs)}{\min\,\{E(fi),E(fs)\}}\right\} \qquad (12)$$

In 2016, Fuzzy Mutual Information-based Feature Selection with Non-Dominated solution (FMIFS-ND) was proposed by N. hoque [18]. The FMIFS-ND selects the features using feature-class fuzzy mutual information and feature-feature fuzzy mutual information.

In 2016, Nguyen Xuan Vinh et. al [12] proposed relaxMRMR. The relaxMRMR estimates relevancy (I(fi; C), dependency(I(fi; fs)), second order interaction (MI(fi ; fi/ft)) and loss-relevant redundancy (I(fi; ft/C)). The three forms of relaxMRMR are defined in equations (13 – 15) as Form-0:

$$max\left\{MI\,(fi\,;C) - \frac{1}{|S|}\sum\nolimits_{fs\,\epsilon\,S}\ \left\{MI\,(fi\,;fs) + \right.\right.$$
$$ft{\in}St{\neq}sMI\,(fi\,;fs|ft\,) + ft\,{\in}S\,M\,I\,(fi\,;ft|C) \qquad (13)$$

Form 1:

$$max\left\{MI\,(fi\,;C) - \frac{1}{|S|}\sum\nolimits_{fs\,\in S}\ MI\,(fi\,;fs) + \right.$$
$$1|S|\ fs\in SMI\ \ fi\,;fsC{-}\ \ 1Sfs\in Sft\in Ss{\neq}tMI\,(fi\,;fs|ft)$$
(14)

Form 2:

$$max\left\{MI\,(fi\,;C) - \frac{1}{|S|}\sum_{fs\,\in S} MI\,(fi\,;fs) + \frac{1}{|S|}\sum_{fs\,\in S} MI\,(fi\,;fs\,|C) - \frac{1}{|S||S-1|}\sum_{fs\,\in\,S}\sum_{\substack{ft\,\in S\\ t\neq s}} MI\,(fi;ft|fs)\right\} \quad (15)$$

In 2016 pascoal et al. [14] proposed maxMIFS which extracts the optimal features with less computational overhead. The equation (16) defines the maxMIFS as

$$\max\{MI\,(C\,;fi) - \max\{MI(\,fi,fs\,)\}\} \qquad (16)$$

We proposed new version of MIFS called simplified mutual information based feature selection (SMIFS) which uses only a candidate feature, class label and recently selected feature to extract the next feature. The selected subset of features is mapped to the five class target classification. SMIFS is discussed in the following section.

3. SIMPLIFIED MUTUAL INFORMATION BASED FEATURE SELECTION (SMIFS).

The literature covers different feature selection methods using mutual information. The computational overhead is high in most of the methods. We proposed computationally efficient Simplified Mutual Information based Feature Selection (SMIFS) algorithm. The SMIFS initially considers all the features of the KDD CUP 99 dataset. It applies forward selection process and extracts the features. The first feature is selected from the given feature set which maximizes the mutual information between candidate feature and the class label. Next feature is extracted by finding the relevance I(C ; fi) and dependency I(fi ; fs). Here fs is the recently selected feature, fi is the candidate feature from given input set of features (F). In each iteration, one feature is selected based on the maximum value produced in equation (17) and placed into the selected feature subset (S) and on this subset we apply multilayer perceptron. This process is continued if the classification accuracy is increasing otherwise we stop the feature selection.

$$\max\{\,MI\,(\,C\,;\,fi) - \,MI\,(\,fi\,;fs)\} \qquad (17)$$

The proposed algorithm is presented in fig 2.

```
Algorithm: SMIFS
Input: Set of all features from KDD CUP 99 data set.
Output: Optimal sub set of relevant features (S)
Procedure:
1. Initialize F= set of all features of KDD CUP 99 data set and S=∅.
2. Calculate the relevancy between the class label and a candidate feature ($f_i$) from F.
   i.e., calculate I( C ; $f_i$)
3. Select the feature fi which gives maximum among the MI( C ; fi), and place this feature into S and remove it from F.    F= F-{$f_i$} and S=S ∪ $f_{i.}$
4. Apply A forward Selection procedure ( A Greedy selection Approach):
      i. calculate the relevancy MI(C ; $f_i$) and dependency MI($f_i$ ; $f_s$).
      ii, find the maximum value using equation (17).
      iii. Select that feature and marked it as selected.
   F= F-{$f_i$} and S=S ∪ $f_{i.}$
5. Repeat the step four until features of S gives high accuracy when S is applied to classifier.
```

In SMIFS only recently selected feature is used to extract the next feature. The order and relevant features also affects the performance of the classifier.

4. EXPERIMENTAL SETUP AND RESULTS

The proposed IDS model uses SMIFS for feature selection and multi layer perceptron as classifier. The proposed model consists of four stages as shown in fig 3. In first stage, data is gathered and divided into train and test data. In our model, KDD CUP 99 data set is used. KDD CUP 99 data set is available in various sizes for training and test data separately. The data set consists of 41 candidate features and one class label. Yinhui Li et.al categorizes [2] the 41 features, 9 features are basic features of individual TCP connection (duration, protocol_type, service etc.,), 13 features are domain knowledge features (hot, logged_in, root_shell etc.,), 9 features are traffic features computed by two second time window (count, serror_rate, srv_count etc.,), and remaining features are transportation feature of target host. In second stage preprocessing is done on the features. In this all non numeric features are transformed to numeric by appropriate functions and also the missing values are imputed. The features V20 and V22 values are zeros and these two are removed from the data set. In stage three, we have estimated the dependency between target class label and the set of features of given data sets using proposed SMIFS of the proposed model. In the first level we build a two class predictive model which categorizes given data into normal and attack. In the second level predictive model is a five class classification model and the classes are normal, dos, probe, r2l and u2r. In the third level we build another model which classifies only the attacks. In four class classification model, the class labels are dos, probe, r2l and u2r. Each time new feature is selected and placed in optimal feature subset. After each feature selection, feature subset is trained using multi layer perceptron with 10-fold cross validation is during the training the model.

Artificial Neural Networks (ANN) is computing systems inspired from the biological neural networks of human and animal brains. In our model shown in figure 2, two types of multilayered neural networks are constructed to classify the data. First model is to classify the data into 5 classes (normal, dos, probe, r2l and u2r) and another model is to classify the attacks data only.

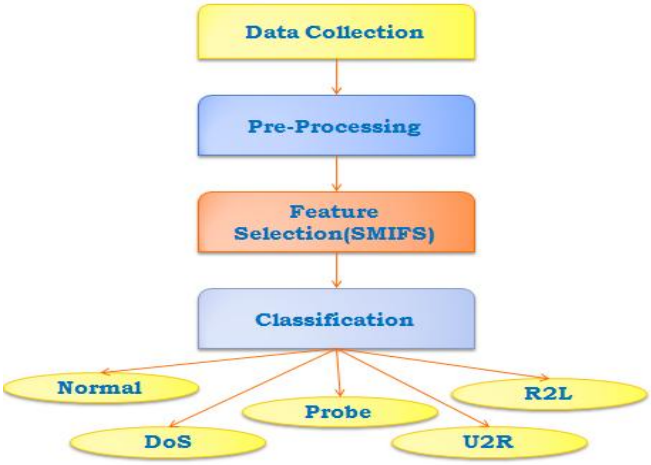

Fig 3: Stages in IDS model using SMIFS and Multi layered perception(5-class classification).

The experiments run in Intel core i4 2093 GHz processor computer with 6 GB RAM and windows 64-bit operating system. The code for the experiments is written in R language and used some of the inbuilt functions and libraries to develop the model.

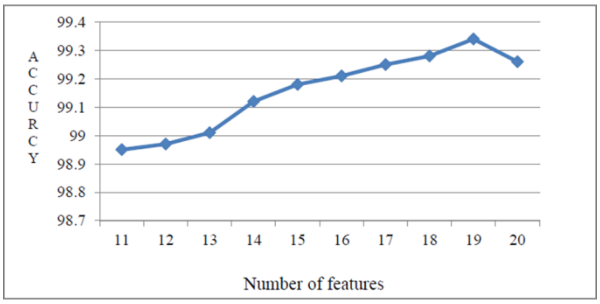

Fig 4: Accuracy of 2-class prediction model with different number of subset features.

After every feature selection using SMIFS, feature subset is trained using two models. The results obtained from the experiments are displayed in table 1 and table 2. For 2 class predictions model the system accuracy is 99.34% with 19 features, for 5 class model the system accuracy is 99.03% with 13 features and 99.563% and for the 4 class attack classification model with 11 features only.

Table 1: Comparison of Accuracy with model with different features

No. of Features selected	Subset of selected features	Accuracy
9	5,9,23,22,24,12,35,37,3	98.21
10	5,9,23,22,24,12,35,37,3,6	98.66
11	5,9,23,22,24,12,35,37,3,6,32	98.74
12	5,9,23,22,24,12,35,37,3,6,32,36	98.82
13	**5,9,23,22,24,12,35,37,3,6,32,36**	**99.03**
14	5,9,23,22,24,12,35,37,3,6,32,36,2	98.75
15	5,9,23,22,24,12,35,37,3,6,32,36,2,31	98.63

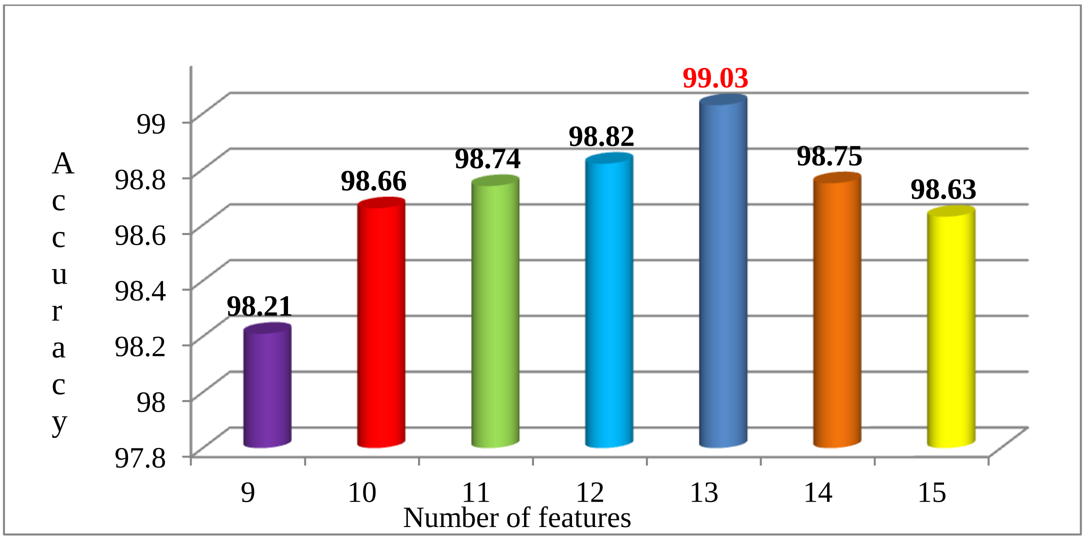

Fig 5: Comparison of accuracy with 5- class model using multilayered neural networks

Table 2 presents the accuracy of the model with different number of inputs to the multilayered neural network. When number of features are 11 out of 41 features of the attack data set of KDD CUP 99 and the model is achieved approximately 99.6% of accuracy. So, we concluded that best features for proposed multilayered neural network with SMIFS is 11 for the categorization of attack data.

Table 2: Results of multilayered neural network on attack data with order of features selection

No. of Features selected	Subset of selected features	Accuracy
9	3,14,5,15,23,22,24,37,35	99.368
10	3,14,5,15,23,22,24,37,35,32	99.442
11	**3,14,5,15,23,22,24,37,35,32,30**	**99.563**
12	3,14,5,15,23,22,24,37,35,32,30,12	99.352
13	3,14,5,15,23,22,24,37,35,32,30,12,30	99.194

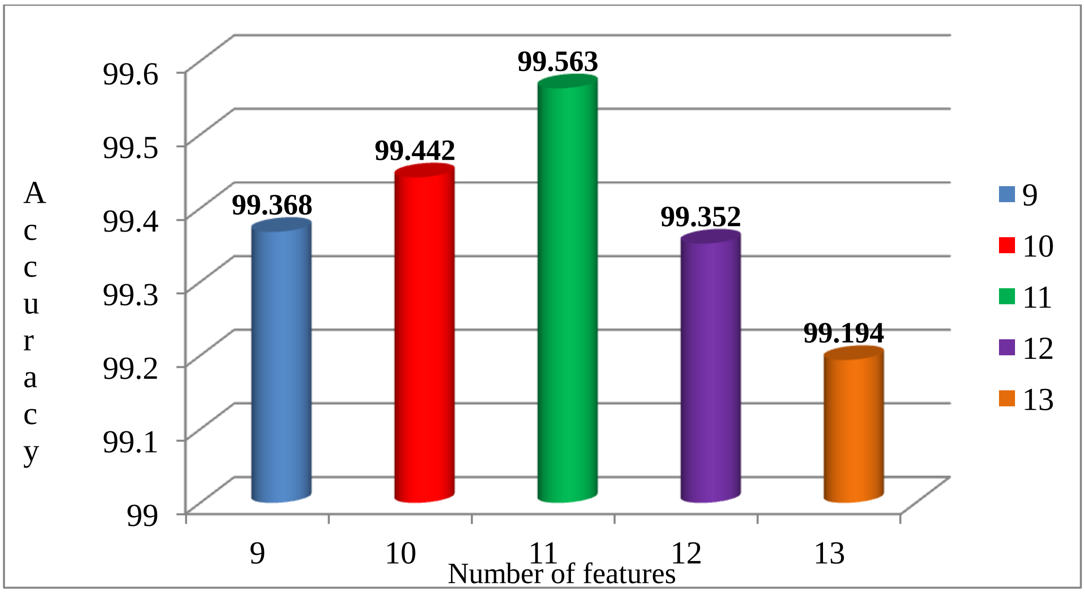

Fig 6: Comparison of accuracy with varying size of features of a attack dataset

The time taken to extract the features using proposed SMIFS is less when we compared with the existing feature extraction methods. The Table 3 shows that the time taken to extract the features using different existing algorithms and the proposed algorithm outperforms the existing algorithms.

Table 3: Comparison of Feature Selection mechanisms

S. No	Feature selection Method	Time for each feature extraction in sec
1	MICC	1.327
2	NMIFS	1.246
3	relaxMRMR	1.458
4	FMIFS-ND	1.378
5	maxMIFS	1.162
6	SMIFS	1.022

We built multilayer neural network predictive model on the extracted features with two-class, four-class and five-class classifications and the results are presented in table 4. The results shows that the accuracy of SMIFS+NN model is almost similar to the other models with less number of features.

Table 4: Comparison of results with different feature selection methods using multilayer neural networks

Feature Selection Method	2-class classifier		5-class classifier		4-class classifier	
	# of features selected	Accuracy	# of features selected	Accuracy	# of features selected	Accuracy
SMIFS + NN	19	99.34	13	99.03	11	99.56
FMIFS + NN	21	99.26	13	99.12	10	99.48
MIFS+ NN	25	99.32	15	98.89	12	99.55
NMIFS +NN	20	99.39	14	98.62	11	99.47
MMFIS + NN	22	99.08	13	99.17	12	99.62

5. CONCLUSION

In this paper, we proposed SMIFS algorithm to extract the useful features from the given data set. This algorithm is computationally efficient comparing with other feature extraction algorithms. The extracted features are feed into the multilayer neural network predictive model. The model is run on 2-class classification, 4-class classification and 5-class classification. The 2-class classifier considers only normal and attack as the classes. The 4-class classifier considers attack as dos, probe, u2r and r2l as classes. The 5-class classifier considers normal, dos, probe, u2r and r2l as classes. The experimental results prove that the proposed SMIFS+NN outperform the other existing mutual information based feature extraction algorithms.

REFERENCES:

1. Mohammed A Ambusaidi, Xianglian He, Priyadarsi Nanda, and Zhiyuan Tan:" Building an Intruison Detection System using a filter based feature selection algorithm"- IEEE Transaction on computers Vol.no November 2014.
2. Yinhui Li, Jingho Xia, Silan Zhang, Jiakai Yan, Xiaochuan Ai and Kuobin Dai:" An efficient Intrsuion Detection System based on Support Vector Machines and gradually feature removal method"-Elsevier-Expert system with Applications-2012
3. Levent Koc, Thomas A Mazzuchi, and Shahram Sarkani: A Network IDS based a Hidden Naïve Bayes Multi Class Classifier-Expert System with Applications 39(2012)-Elsevier.
4. Fangjun Kuang, Weihong Xu, and Siyomg Zhang "A novel hybrid KPCA and SVM with GA model for Intrusion Detection"-Elsevier Applied soft Computing 2014.
5. D. P. Gaikwad and Ravindra C. Thool: IDS using Bagging Ensemble method of Machine Learning- 2015 International conference on Computing Communication Control and Automation.
6. D Huang and Tommy W S Chow: Searching optimal feature subset using mutual information-European Symposium on Artificial Neural Networks, April 2003.
7. Tommy W S Chow and D. Huang: Estimating Optimal Feature Subsets Using Efficient Estimation of High-Dimensional Mutual Information-IEEE transactions on Neural Networks, vol, 16 No. 1, January 2005.
8. Huawen Liu, Yuchang Mo and Jianmin Zhao: "Conditional Dynamic mutual information based Feature Selection-Computing and Informatics. Vol 31,2012.
9. H. Peng, F. Long and C. Ding- Feature selection based on mutual information criteria of max- dependency, max-relevance and min-redundency- IEEE transaction on pattern analysis and Machine intelligence-vol 27(2005).
10. Roberto Battiti: Using Mutual Information for Selecting Features in Supervised Neural Net Learning-IEEE transactions on Neural Networks, vol. 5 No. 4 July 1994.
11. Nojun Kwak and Chong – Ho Choi: Input Feature Selection for Classification problems -IEEE Transactions on neural Networks, vol. 12 no. 1, January 2002.
12. Nguyen Xuan Vinh, Shuo Zhou, Teffrey Chan, James Bailey: Can high Order Dependencies improve mutual information based feature selection-Pattern Recognization 53(2016)-Elsevier.
13. Pablo A. Estevex, Michel Tesmet Claudio A. Perez and Jacek M. Zurada: Normalized Mutual Information Feature Selelction-IEEE Transactions on Neural Networks, vol. 20, no 2, January 2009
14. Claudia Pascoal, M. Rosario Oliveria, Antonio Pacheco and Rui Valadas:" Theoretical evalution of feature Selection methods based on mutual information"-Neurocomputing 2016.
15. Shannon .C. E., "A Mathematical Theory of communication", Bell System Technical journal, July 1948, Oct. 1948.
16. C. E . Shannon, " Communication Theory of Secrecy Systems" Bell System Technical Journal, Oct. 1949.

17. Huang J. J, Lv N, Li Sq and Cai Yz: Feature Selection for Classificatory analysis based on Information-theoretic criteria-Acta Automatica Sinica 2008.
18. N. Hoque, D. K. Bhattacharyya, and J.K. Kalita-" MIFS-ND: A mutual information based feature selection method", Expert System with Applications,41(2014)-Elsevier.
19. Craig H. Rowland:"Intrusion Detection System"-Google patents,2002.
20. Robin Sommer and Vern Paxson:" Outside the closed world: On Using Machine Learning for Network Intrusion Detection"- 2010 IEEE symposium on Security and Privacy.
21. Srinivas M, Andrew H. Sung: " Feature ranking and Selection for Intrusion Detection System using support vector machines" -2002.
22. gary Stein, Bing Chen, Annie S. Wu, and Kien A. Hue :"Decision Tree classifier for Network Intrusion Detection with GA-based Feature Selection"-2005.
23. Cize Thomas, Vishwas Sharma, N. Balakrishnan:"usefulness of DARPA dataset for Intrusion Detection Evaluation
24. Jana Novovicova, Petr Somol, Michal Haindl and Pavel Pudil: Conditional Mutual Information based feature selection for Classification Task. Springer 2007.
25. Huawen Liu, Yuchang Mo, and Jianmin Zaho:"Conditional Dynamic Mutual Information based Feature Seelction- Computing and Informatics, vol. 21, 2012-Elsevier.
26. Fatemeh Amiri, Mohammad Rezael Yousefi, Caro Lucus, Azadeh Shakery, Nasser Yazdani : Mutual information based feature selection for intrusion detection systems - Journal of Network and Computer applications- Elsevier (2011).
27. S. Cang , H. Yu,-Mutual information based feature selection for classification problems- Decision support systems-54(1),(2012) 691-698.
28. Mohammed A. Ambusaidi: Using Mutual Information for Feature Selection in Network Intrusion Detection System-Proceedings of the Third International Conference on Digital Security and Forensics (DigitalSec), Kuala Lumpur, Malaysia, 2016.