ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

The Framework of Intrusion Detection System Using Flexible Filter-Based Feature Selection Algorithm

Pooja Parbhanikar, K.S.Korabu

M. E Student, Department of IT, SCOE, Pune, India

Professor, Department of IT, SCOE, Pune, India

ABSTRACT: Redundant and inapplicablefeatures in information have caused a long haul issuein network traffic classification. These highlights back off the procedure of arrangement as well as keep a classifier from settling on precise choices, particularly when adapting to huge information.Mutualinformationbased mostlyalgorithmic program has used that analytically selects the best feature for classification. This mutual informationbased mostly feature selectionalgorithmic programwill handle dependent informationoptionslinearly and nonlinearly. Its effectiveness is evaluated within the cases of network intrusion detection. Associate in Network Intrusion Detection System (IDS), named Least Square Support Vector Machine based mostly IDS (LSSVM-IDS), is madeexploitation the featureselite by theplanned feature selectionalgorithmic program. The performance of LSSVM-IDS is evaluated intrusion detection analysis datasets, particularly KDD Cup 99 and NSL-KDD dataset. The contribution work is, replacing the classification algorithm as Ripper algorithm.An existing system uses LS-SVM classifiers for classification but as compare to Ripper classifier with association rules mining to select most valuable features of a dataset. Firstly, building rules using Ripper classifier, then assigning ranks to features by using these rules based on support and confidence. Using Ripper classifier algorithm accuracy of classification is high and it is to identify important reduced input features in building IDS that is computationally efficient and effective.

KEYWORDS: FeatureSelection,Intrusion Detection, Least Square Support Vector Machine,Linear CorrelationCoefficient,Mutual Information, Ripper

I. INTRODUCTION

Over the past decades, Internet and computer systems have raised numerous security issues due to the explosive use of networks. Any malicious intrusion or attack on the network may give rise to serious disasters. Intrusion is a malicious, harmful entity which is responsible for network attack. They violate integrity, confidentiality and availability of a system resource. In this case, system is failed to respond for data stolen or being lost. So, Intrusion Detection Systems (IDSs) are must to decrease the serious influence of these attacks. Intrusion Detection System is defined as the system or software tool to detect unauthorized access to a network or computer system.

IDS is capable of detecting all types attack like malicious, harmful attack, vulnerability, data driven attacks, host based attacks for example privilege violation, sensitive file access, unauthorized logins and malwares. Then need IDS once have firewall because the networks having firewall were not designed to detect attack at network layer and application layer such as worms, viruses, Denial of services (DoS), distributed denial of services (DDoS) and Trojans. The work of firewall is to stop external traffic from entering in the internal network.

The intrusions are like viruses, worms, Trojans, or network attacks like unauthorized login, access of sensitive files, or data driven attacks on application. The intrusion violates the integrity, confidentiality and availability. Because

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

of this system is unable to respond or access is denied. Thus intrusion detection means detection of unauthorized use of system or an attack on a system or network. The Intrusion detection system (IDS) is a hardware or software tool to detect these activities. Feature selection is a technique for eliminating irrelevant and redundant features and selecting the most optimal subset of features that produce a better characterization of patterns belonging to different classes. Methods for feature selection are generally classified into filter and wrapper methods. This paper focus on filter methods for IDS.

Motivation:

1. The Detection accuracy of anomaly system should maximize.
2. The false positive rate should minimum.
3. The detector generation time should less.

Objectives:

The goal of proposed LSSVMclassification algorithm is to maximize performance in terms of classification accuracy, detection rate, false positive rate and F-measure.

The objectives of the proposed application are as follows:

1. To study existing Network Intrusion Detection Systems (NIDSs) and types of NIDSs.
2. To study various machine learning algorithms like Bayesian networks, Neural networks, fuzzy logic, outlier detection and genetic algorithm.
3. To study current filter-based feature selection approach for detection of intrusion attacks using Flexible mutual information based feature selection (FMIFS) and Flexible Linear Correlation Coefficient based Feature Selection (FLCFS) algorithm.
4. To analyze the experimental results of proposed LSSVM+FMIFS and LSSVM+FLCFS algorithms for intrusion detection system.
5. To propose a new integrated approach for network intrusion detection using JRipper classifier algorithm, to reduce detector generation time and also to increase its adaptability and flexibility the studied parameter value selected automatically according to the used training dataset.
6. To compare the experimental results of LSSVM and Ripper classifier for network intrusion detection algorithm which gives results as accuracy of classification is high.

II. EXISTING SYSTEM

The current network traffic data, which are often huge in size, present a major challenge to IDSs These “big data” slow down the entire detection process and may lead to unsatisfactory classification accuracy due to the computational difficulties in handling such data. Classifying a huge amount of data usually causes many mathematical difficulties which then lead to higher computational complexity. As a well-known intrusion evaluation dataset, KDD Cup 99 dataset is a typical example of large-scale datasets. This dataset consists of more than five million of training samples and two million of testing samples respectively. Such a large scale dataset retards the building and testing processes of a classifier, or makes the classifier unable to perform due to system failures caused by insufficient memory. Furthermore, large-scale datasets usually contain noisy, redundant, or uninformative features which present critical challenges to knowledge discovery and data modeling.

Disadvantages:

Computer systems and internet have become a major part of the critical system. The current network traffic data, which are often huge in size, present a major challenge to IDSs. These “big data” slow down the entire detection process and may lead to unsatisfactory classification accuracy due to the computational difficulties in handling such data. Classifying a huge amount of data usually causes many mathematical difficulties which then lead to higher computational complexity.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

III. REVIEW OF LITERATURE

The existing works remain incapable of fully protecting internet applications and computer networks against the threats from ever-advancing cyber-attack techniques such as DoS attack and computer malware. The traditional security techniques, as the first line of security defense, such as user authentication, firewall and data encryption, are insufficient to fully cover the entire landscape of network security while facing challenges from ever-evolving intrusion skills and techniques. The network intrusion detection system applies feature selection methods like filter, wrapper based method. These are describes below papers:

The paper [1] proposes a more sophisticated anomaly based system for detecting DoS attacks. The former technique helps extract the correlations between individual pairs of two distinct features within each network traffic record and offers more accurate characterization for network traffic behaviors. Advantages are: Able to cope with high speed network segments. Proposed detection system achieves maximum 99.95% detection accuracy on KDD Cup 99 data set and 90.12% detection accuracy on ISCX 2012 IDS evaluation data set. The paper [2] proposes Half-partition strategy of selecting and retaining non-support vectors of the current increment of classification-named as Candidate Support Vectors (CSV) - which are likely to become support vectors in the next increment of classification. The proposed Incremental Support Vector Machine is the selection of Candidate Support Vectors. Here, two methods of selecting CSVs are presented: (1) Improved Concentric Circle method; and (2) Half-partition strategy. Advantages are: Proposed system is more efficient and faster Support Vector selection method. The proposed method has better detection rate and false alarm rate as well as acceptable amount of learning time. Disadvantages are: The Half-partition strategy actually discards almost half the data points lying farther than the class center from the hyper plane.

A new hybrid intrusion detection method [3] that hierarchically integrates a misuse detection model and an anomaly detection model in a decomposition structure is proposed.The DT and 1-class SVM algorithms that are required in order to build the misuse detection model and anomaly detection model. Advantages are: C4.5 decision tree (DT) was used to create the misuse detection model that is used to decompose the normal training data into smaller subsets. 1-class SVM was used to create an anomaly detection model in each decomposed region. Increase the IDS in terms of detection performance for unknown attacks and detection speed. Disadvantages are: The C4.5 algorithm in order to decompose the normal data evenly into each subset with degrading the misuse detection performance.

The paper [4] presents a different, traffic-aware, modular approach in the design of FPGA-based NIDS. Instead of purely splitting traffic across equivalent modules, then classify and group homogeneous traffic, and dispatch it to differently capable hardware blocks, each supporting a (smaller) rule set tailored to the specific traffic category. Advantages are: Traffic awareness permits to fine tune the amount of HW resources dedicated to each traffic category. Each string matching engine supports only a subset of IDS rules, and thus optimization of its HW implementation appears more effective. Disadvantages are: The IDS rules which are by far more complex (i.e. resource consuming) in terms of HW implementation.

In [5] paper, develop PLSSVM, novel IDS which uses a reformulation of Support Vector Machine (SVM), called least square SVM (LSSVM), for modeling the system. To build lightweight IDS, two dependency-based feature selection algorithms with different evaluation functions have been proposed in this work: linear correlation-based feature selection (LCFS) and modified mutual information-based feature selection (MMIFS). Advantages are: Modified mutual information-based feature selection method (MMIFS) is a feature selection method with maximum relevancy and minimum redundancy. Higher accuracy. Disadvantages are: Since MMIFS and FFSA use more information to select features. The paper [6] proposed an SVM-based network intrusion detection system with BIRCH hierarchical clustering for data preprocessing. The BIRCH hierarchical clustering could provide highly qualified, abstracted and reduced datasets, instead of original large dataset, to the SVM training. Advantages are: The proposed system could

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

greatly shorten the training time. Achieve better detection performance in the resultant SVM classifier. Disadvantages are: This system showed superior performance in DoS and Probe attacks, though it was not the best for U2R and R2L attacks.

In [7] paper, presented a framework for Distributed Intrusion Detection Systems (DIDS) using several soft computing paradigms. Proposes a hybrid architecture involving ensemble and base classifiers for intrusion detection. Advantages are: The fuzzy classifier (FR2) gave 100% accuracy for all attack types. Feature reduction to model lightweight intrusion detection systems. The lightweight SCIDS would be useful for MANET/distributed systems, the heavy weight SCIDS would be ideal for conventional static networks, wireless base stations etc. Disadvantages are: The number of possible fuzzy if-then rules exponentially increases with the dimensionality of the pattern space. The paper [8] presents a comparative study of using support vector machines (SVMs), multivariate adaptive regression splines (MARSs) and linear genetic programs (LGPs) for intrusion detection. Address the related issue of ranking the importance of input features, which itself is a problem of great interest. Advantages are: More accurate detection. Faster feature selection. The testing time decreases.

In [9] paper, the performance of two feature selection algorithms involving Bayesian networks (BN) and Classification and Regression Trees (CART) and an ensemble of BN and CART.Proposes hybrid architecture for combining different feature selection algorithms for real world intrusion detection (or attribute) estimation of other types of user-generated content. Advantages are: To reduce the amount of data directly processed by the IDS. Decreases storage requirements, reduces processing time and improves the detection rate. Combine the redundant and complementary classifier is to increase robustness, accuracy, and better overall generalization. Disadvantages are: Less accurate base classifiers particularly for the detection of U2R type of attacks.

The paper [10] represents the use of the mutual information (MI for short) to evaluate the “information content” of each individual feature with regard to the output class. The building blocks of the MIFS algorithm, where the features are selected in a “greedy” manner, ranking them according to their MI with respect to the class discounted by a term that takes the mutual dependencies into account. Advantages are: The irrelevant features are eliminated from the beginning and fast informative feedback about the relevance and dependencies of the different features is available .Low computational complexity. Disadvantages are: The availability of sufficient information does not guarantee the convergence of a neural net training algorithm to a satisfactory performance level.

IV. PROPOSED SYSTEM

Intrusion detection system (IDS) can be software or hardware that monitors for intrusions and anomalies from the environment it is set to guard. In general the IDS is a security monitoring tool like a firewall that tries to detect and possibly prevent malicious activity. Two main techniques for intrusion detection exist based on what they can detect. These two techniques are misuse detection and anomaly detection. Misuse detection and anomaly detection systems can be further divided into two groups based on the detection method; into behavior based and into knowledge based IDS. Behavior based IDS monitor behavior deviations of the system in order to detect intrusions and anomalies. Knowledge based IDS monitors a system using patterns of known intrusions.

The framework of the proposed intrusion detection system is comprised of four main phases:
(1) Data collection, where sequences of network packets are collected,
(2) Data preprocessing, where training and test data are preprocessed and important features that can distinguish one class from the others are selected,
(3) Classifier training, where the model for classification is trained using LS-SVM, and
(4) Attack recognition, where the trained classifier is used to detect intrusions on the test data.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

The fig.1 shows the proposed system architecture that describes how the system works below:

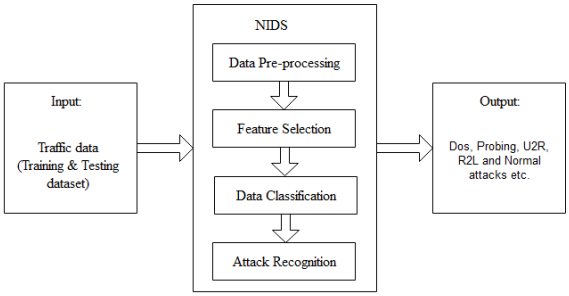

Fig.1 Proposed System Architecture

1] Data Collection

Data collection is the first and a critical step to intrusion detection. The type of data source and the location where data is collected from are two determinate factors in the design and the effectiveness of IDS. To provide the best suited protection for the targeted host or networks, this study proposes network-based IDS to test the proposed approaches. The proposed IDS run on the nearest router to the victim(s) and monitor the inbound network traffic. During the training stage, the collected data samples are categorized with respect to the transport/Internet layer protocols and are labeled against the domain knowledge. However, the data collected in the test stage are categorized according to the protocol types only.

2] Data Preprocessing

The data obtained during the phase of data collection are first processed to generate the basic features such as the ones in KDD Cup 99 dataset. This phase contains three main stages shown as follows.

2.1 Data transferring

The trained classifier requires each record in the input data to be represented as a vector of real number. Thus, every symbolic feature in a dataset is first converted into a numerical value. For example, the KDD CUP 99 dataset contains numerical as well as symbolic features. These symbolic features include the type of protocol (i.e., TCP, UDP and ICMP), service type (e.g., HTTP, FTP, Telnet and so on) and TCP status flag (e.g., SF, REJ and so on). The method simply replaces the values of the categorical attributes with numeric values.

2.2 Data normalization

An essential step of data preprocessing after transferring all symbolic attributes into numerical values is normalization. Data normalization is a process of scaling the value of each attribute into a well-proportioned range, so that the bias in favor of features with greater values is eliminated from the dataset. Every feature within each record is normalized by the respective maximum value and falls into the same range of [0-1].

3] Feature selection

Even though every connection in a dataset is represented by various features, not all of these features are needed to build IDS. Therefore, it is important to identify the most informative features of traffic data to achieve higher performance. The Flexible Mutual Information based Feature Selection (FMIFS) is designed to reduce the number of features. The Flexible Linear Correlation Coefficient based Feature Selection (FLCFS) is designed to select a feature that maximizes correlation and to eliminate irrelevant and redundant features. However, the proposed feature selection algorithms can only rank features in terms of their relevance but they cannot reveal the best number of features that are

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

needed to train a classifier. To do so, the technique first utilizes the proposed feature selection algorithm to rank all features based on their importance to the classification processes.

4] Classification

The optimal subset of features is selected, for all classes, five LS-SVM classifiers need to be applied on testing dataset. Each classifier distinguishes one class of records from the others. For example the classifier of Normal class distinguishes Normal data from non-Normal (All types of attacks). The DoS class distinguishes DoS traffic from non-DoS data (including Normal, Probe, R2L and U2R instances) and so on. The five LS-SVM classifiers are then combined to build the intrusion detection model to distinguish all different classes. The proposed algorithm Ripper is applied on testing dataset to reduce the time of intrusion classification.

Advantages:

1. The training and testing sets contains suitable number of records to make it easy to execute experiments on whole data set. There is no need to select small area randomly.
2. The experimental results are consistent and comfortable.
3. It does not contain duplicate data in the training and testing set. Thus the results are more accurate than the method which has better detection rates using frequent records.
4. The intrusion classification rates vary according to different machine learning algorithm. So it is useful for efficient and accurate detection of different learning techniques.

V. MATHEMATICAL MODEL

1. Preprocessing:

In this step, training data source (T) is normalized to be ready for processing by using following steps:

$$T_{norm} = \{\frac{T-\mu_T}{\sigma_T}, \sigma_T \neq 0 \; and \; T - \mu_T, \sigma_T = 0 \qquad (1)$$

Where,

$$\mathbf{T} = \{x_{ij} \mid i = 1, 2, 3....mandj = 1, 2, 3....n\}$$
$$\mu_T = \{\mu_j \mid j = 1, 2, 3....n\}$$
$$\sigma_T = \{\sigma_j \mid j = 1, 2, 3, ..., n\}$$

T is m samples with n column attributes; x_{ij} is the jth column attribute in ith sample, μ_T and μ_T are 1*n matrix which are the training data mean and standard deviation respectively for each of the n attributes. Test dataset (TS) which is used to measure detection accuracy is normalized using the same μ_T and μ_T as follows:

$$TS_{norm} = \frac{(TS - \mu_T)}{\sigma_T}, \sigma_T \neq 0 and TS - \mu_T, \sigma_T = 0 \qquad (2)$$

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

2. Feature Selection:

Given two continuous random variables $U = \{u_1, u_2, \dots, u_d\}$ and $V = \{v_1, v_2, \dots, v_d\}$, where d is the total number of samples, the mutual information between U and V is given below:

$$I(U;V) = H(U) + H(V) - H(U,V) \quad (3)$$

Where, H(U) and H(V) are the information entropies of U and V. The information entropies are the measures of uncertainties of the random variables U and V, where $H(U) = -\int_u p(u) \log p(u)\, du$ and $H(V) = -\int_v p(v) \log p(v)\, dv$ respectively.

The joint entropy of U and V is defined as,

$$H(U,V) = -\int_u \int_v p(u,v) \log p(u,v)\, dudv \quad (4)$$

Therefore, to quantify the amount of knowledge on variable U provided by variable V, which is known as mutual information, (5) is used.

$$I(U;V) = \int_u \int_v p(u,v)\, log \frac{p(u,v)}{p(u)p(v)}\, dudv \quad (5)$$

Equation (6) shows a new formulation of the feature selection criterion involved, which is intended to select a feature from an initial input feature set that maximizes $I(C; f_i)$ and minimizes the average of redundancy MRs simultaneously.

$$G_{MI} = \underset{f_i \in F}{argmax}(I(C;f_i) - \frac{1}{|S|}\sum_{f_s \in S} MR) \quad (6)$$

Flexible Linear Correlation Coefficient based Feature Selection (FLCFS) Algorithm is designed to select a feature that maximizes G_{corr} in Equation (7) and to eliminate irrelevant and redundant features.

$$G_{corr} = \underset{f_i \in F}{argmax}(corr(C;f_i) - \frac{1}{|S|}\sum_{f_s \in S} \frac{corr(f_i,f_s)}{corr(C,f_i)}) \quad (7)$$

Algorithms:
1] Attack classification based on LS-SVM Algorithm
Input: LS-SVM Normal Classifier, selected features (normal class), an observed data item x
Output: L_x- the classification label of x
Process:
Step 1: **Begin**
Step 2: $L_x \leftarrow$ classification of x with LS-SVM of DoS class
Step 3: **if** L_x== "DoS" **then**
Step 4: Return L_x
Step 5: **else**
Step 6: $L_x \leftarrow$ classification of x with LS-SVM of Probe class
Step 7: **if** L_x== "Probe" **then**
Step 8: Return L_x
Step 9: **else**
Step 10: $L_x \leftarrow$ classification of x with LS-SVM of R2L class

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

Step 11: **if** L_x== "R2L" **then**
Step 12: Return L_x
Step 12: **else**
Step 13: L_x == "U2R";
Step 14: Return L_x
Step 15: **end**
Step 16:**end**
Step 17: **end**
Step 18: **end**

2] Ripper algorithm:

1. Start from an empty rule: {} => class
2. Add conjuncts that maximizes FOIL's information gain measure:

a. R0: {} => class (initial rule)
b. R1: {A} => class (rule after adding conjunct)
c. Gain(R0, R1) = t [log (p1/(p1+n1)) – log (p0/(p0 + n0))]

where t: number of positive instances covered by both R0 and R1

- p0: number of positive instances covered by R0
- n0: number of negative instances covered by R0
- p1: number of positive instances covered by R1
- n1: number of negative instances covered by R1

VI. EXPERIMENT RESULT

The NSL-KDD dataset is modified version of KDD Cup 99 to overcome some problems in KDD Cup 99 like performance evaluation of system. NSL-KDD is publicly available for researchers. The NSL-KDD dataset contains total 41 attributes which are given below:

Table I The NSL-KDD Dataset Attributes

Total Attributes		
duration	su_attempted	same_srv_rate
protocol_type	num_root	diff_srv_rate
service	num_file_creation	srv_diff_host_rate
flag	Num_shells	dst_host_count
Src_byte	Num_access_file	dst_host_srv_count
Dst_byte	Num_outbound_cmds	dst_host_same_srv_rate
land	is_host_login	dst_host_diff_srv_rate
wrongfragment	is_gust_login	dst_hot_same_src_port_rate
urgent	count	dst_host_srv_diffhost_rate
hot	srv_count	dst_host_serror_rate
num_failed_login	serror_rate	dst_host_srv_serror_rate
logged_in	srv_serror_rate	dst_host_rerror_rate
num_compromised	rerror_rate	dst_host_srv_rerror_rate
root_shell	srv_rerror_rate	class

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

For experimental set up, use Windows 7 operating system, Intel i5 processor, 4 GB RAM, 200GB Hard disk, Eclipse Luna JDK 7 tool. To calculate the results, NSL KDD data set is used. NSL KDD dataset is a modified version of KDD cup 99. In training dataset, there are 23 types of attack and in testing phase additional 14 attacks are included.

The performance evaluation of anomaly based network intrusion detection system is held using different parameters. The Parameters are Detection Accuracy, False Positive Rate, and Detection Time.

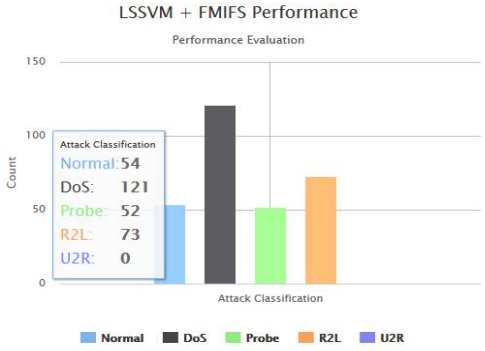

Fig. 2 LSSVM +FMIFS attack classification

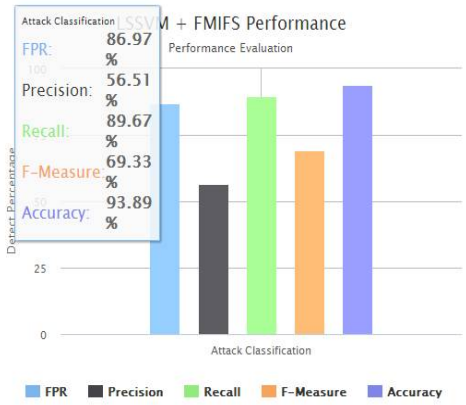

Fig. 3 LSSVM + FMIFS attack classification results

VII. CONCLUSION AND FUTURE WORK

The proposed feature selection algorithm is computationally efficient when it is applied to the LSSVM-IDS. The building (training) and test times consumed by the detection model using FMIFS compared with the detection model using all features. The figure shows that the LSSVM-IDS + FMIFS perform better than LSSVM-IDS with all features on dataset. In this paper, a supervised filter-based feature selection algorithm has been proposed, namely

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

Flexible Mutual Information Feature Selection (FMIFS). FMIFS is an improvement over MIFS and MMIFS. FMIFS suggests a modification to Battiti's algorithm to reduce the redundancy among features. The proposed LSSVM-IDS + FMIFS has shown comparable results with other state-of the-art approaches when using the Corrected Labels sub-dateset of the NSL KDD dataset and tested on Normal, DoS, and Probe classes; it outperforms other detection models when tested on U2R and R2L classes.In future scope, the system will be implemented using another standard dataset either real time or non-real time. By reducing the offline processing time overhead, the online processing time will be minimized.

REFERENCES

[1] Z. Tan, A. Jamdagni, X. He, P. Nanda, L. R. Ping Ren, J. Hu, Detection of denial-of-service attacks based on computer vision techniques, IEEE Transactions on Computers 64 (9) (2015) 2519–2533.
[2] R. Chitrakar, C. Huang, Selection of candidate support vectors in incremental svm for network intrusion detection, Computers & Security 45 (2014) 231–241.
[3] G. Kim, S. Lee, S. Kim, A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, Expert Systems with Applications 41 (4) (2014) 1690–1700.
[4] S. Pontarelli, G. Bianchi, S. Teofili, Traffic-aware design of a highspeed fpga network intrusion detection system, Computers, IEEE Transactions on 62 (11) (2013) 2322–2334.
[5] F. Amiri, M. Rezaei Yousefi, C. Lucas, A. Shakery, N. Yazdani, Mutual information-based feature selection for intrusion detection systems, Journal of Network and Computer Applications 34 (4) (2011) 1184–1199.
[6] S.-J. Horng, M.-Y. Su, Y.-H. Chen, T.-W. Kao, R.-J. Chen, J.-L. Lai, C. D. Perkasa, A novel intrusion detection system based on hierarchical clustering and support vector machines, Expert systems with Applications 38 (1) (2011) 306–313.
[7] A. Abraham, R. Jain, J. Thomas, S. Y. Han, D-scids: Distributed soft computing intrusion detection system, Journal of Network and Computer Applications 30 (1) (2007) 81–98.
[8] S. Mukkamala, A. H. Sung, Significant feature selection using computational intelligent techniques for intrusion detection, in: Advanced Methods for Knowledge Discovery from Complex Data, Springer, 2005, pp. 285–306.
[9] S. Chebrolu, A. Abraham, J. P. Thomas, Feature deduction and ensemble design of intrusion detection systems, Computers & Security 24 (4) (2005) 295–307.
[10] R. Battiti, Using mutual information for selecting features in supervised neural net learning, IEEE Transactions on Neural Networks 5 (4) (1994) 537–550.