Intrusion Detection System using Fuzzy Rough Set Feature Selection and Modified KNN Classifier

Balakrishnan Senthilnayaki[1], Krishnan Venkatalakshmi[2], and Arpputharaj Kannan[1]
[1]Department of Information Science and Technology, College of Engineering, Anna University, Chennai
[2]Departemnt of Electronics and Communication Engineering, University College of Engineering Tindivanam, Anna University, Tindivanam

Abstract: *Intrusion detection systems are used to detect and prevent the attacks in networks and databases. However, the increase in the dimension of the network dataset has become a major problem nowadays. Feature selection is used to reduce the dimension of the attributes present in those huge data sets. Classical Feature selection algorithms are based on Rough set theory, neighborhood rough set theory and fuzzy sets. Rough Set Attribute Reduction Algorithm is one of the major theories used for successfully reducing the attributes by removing redundancies. In this algorithm, significant features are selected data are extracted. In this paper, a new feature selection algorithm is proposed using the Maximum dependence Maximum Significance algorithm. This algorithm is used for selecting the minimal number of attributes of knowledge Discovery and Data (KDD) data set. Moreover, a new K-Nearest Neighborhood based algorithm proposed for classifying data set. This proposed feature selection algorithm considerably reduces the unwanted attributes or features and the classification algorithm finds the type of intrusion effectively. The proposed feature selection and classification algorithms are very efficient in detecting attacks and effectively reduce the false alarm rate.*

Keywords: *Rough set, fuzzy set, feature selection, classifications and intrusion detection.*

Received June 9, 2015; accepted March 9, 2016

1. Introduction

Intrusion detection is necessary in today's computing environment because it is impossible to keep pace with the current and potential threats and vulnerabilities in computing systems. Moreover, the networking technology is constantly changing due to the arrival of web and internet technologies [29]. To make matters worse, threats and vulnerabilities in the environment are also constantly evolving. An Intrusion detection system is used to handle threats and vulnerabilities in the system. Threats occur due to people or groups who have the potential to compromise the system. An intrusion may cause production downtime, sabotage of critical information, and theft of confidential information, cash, or other assets [14].

It may even create negative public relations that may affect a company's growth [3]. Intrusion detection products are able to assist in protecting a company from intrusion by expanding the options available to manage the risk from threats and vulnerabilities. The system can be used to detect an intruder, identify and stop the intruder, support investigations to find out how the intruder got in and stop the exploit from use by future intruders. The correction should be applied across the enterprise to all similar platforms. Intrusion detection products become very powerful in the information security.

In feature selection in Intrusion Detection System (IDS) is also known as variable selection, attribute selection or variable subset selection, is the process of selecting a subset of relevant features for use in model construction.

Redundant features are those which provide no more information than the currently selected features, and irrelevant features provide no useful information in any context. Feature selection techniques are often used in domains where there are many features and comparatively few samples.

Classification is also useful as part of the data analysis process, as it helps to group the data which is important for predicting. Moreover, the choice of evaluation metric heavily influences the algorithm. In this paper, we propose new IDS for enhancing security that utilizes the information on knowledge Discovery and Data (KDD) dataset. The contributions of this paper are as follows.

- We define and select an important feature from the collected dataset. We also suggest a way of removing redundant attributes.
- We provide how to determine the correct user and set the alarm to attackers by using the selected features.
- We propose a new classification algorithm for enhancing the security.

This remainder of this paper is organized as follows. In section 2, related studies are reviewed, and in section 3, an overview of the proposed IDS is given. Section 4 cover feature selection technique, and section 5

discusses the proposed classification algorithm on the experimental results, and in Section 6, the conclusions work is presented.

2. The Related Work

In this section, the related work on feature selection, feature classification, and Intrusion Detection System are reviewed.

2.1. Feature Selection

There are many works in the literature that discuss feature selection [4, 5, 23]. Feature selection is an important technique for selecting the best attributes for a given data set. Literature [5] described a methodology for performing variable selection using Support Vector Machines (SVMs). It explores the feature selection problem through Feature Subset Selection using Expectation-Maximization Clustering (FSSEM) and uses scatter separability and maximum likelihood performance criteria for evaluating candidate feature subsets [4]. Analyzed the feature selection in text domains to make learning efficient [6]. His paper presents a new IDS is proposed optimal genetic algorithm for feature selection and SVM based classification for detecting attack types [27]. Literature [15], proposed system uses the concept of fuzzy-rough feature relevance and significance for finding siginificant and relevant features of real valued data sets.

The feature selection algorithm deals with the statistical method for analyzing the voluminous knowledge Discovery and Data (KDD) cup dataset [25]. The rough set is reliant upon a discredited dataset, i.e. important information may be lost as a result of the dissertation [11]. Proposed a wrapper based feature selection algorithm in order to develop an IDS. Their approach is better for selecting features and provides high detection rate [29].

2.2. Works on Intrusion Detection System

Malny works are present in the literature about IDS [2, 8, 16, 20, 21, 24, 26]. This proposed system is that the deviation from the normal behavior of the user could be easily diagnosed fairly and quickly by the Neural Network (NN) model for IDS [2]. This proposed work explores a prevention technique in intrusion detection system to detect and prevent the intrusions in cloud computing systems [20]. Moradi and Zulkernine [16] presented a new IDS that uses Artificial Neural Network (ANN) for effective intrusion detection. They have taken care in adding new agents in such a way that the failure of one agent does not degrade the overall detection performance of the network. Literature [24] proposed a novel multilevel hierarchical Kohonen network to detect intrusions on networks. Previous literature [8] proposed a new IDS for feature selection using intelligent Conditional Random Field based algorithm. Proposed system is that provide intrusion detection and prevention using fuzzy logic risk analysis technique [21]. This proposed system a new intrusion detection system has been developed for optimal feature selection algorithm selects the important features that reducing the time taken for detecting and classifying the records [26].

2.3. Works on Classification

There are many classification algorithms based on SVM that is found in the literature for IDS. For example, an algorithm called tree structured multiclass SVM has been proposed for classifying data effectively [17]. Onut and Ghorbani [19] presented a feature classification schema for network intrusion detection that intends to provide a better understanding of the features extracted from the network packets. Literature [14] provided a survey on intelligent techniques for feature selection and classification for intrusion detection in networks. The author proposed that enhanced C4.5 decision tree algorithm for IDS [22].

Gondaliya-Tapan and Maninder-Sing [9] implemented an Intrusion Detection System to prevent the attacks in mobile Adhoc networks. An intrusion detection system by applying Genetic Algorithm (GA) to efficiently detect the various types of intrusions [10]. This has been improved to network security today. Security mechanisms are to find the unauthorized users as well as the authorized users [12]. Proposed a novel algorithm for Multiple Adaptive Learning which combines Multiple Kernel Boosting with the Multiple Classification in the Reduced Kernel [7]. Literature [28], proposed a new framework for Analyzing Intrusion Alerts using classification. They carried out the experiments with industrial partners of the British Telecom Security Practice and showed a false positive rate 97%. A new feature selection algorithm based on subsets and used in the decision tree classifier [1]. The support vector data description and kernel principle component analysis for detecting several types of cyber-attacks using classification [18]. Investigated the performance and the detection accuracy of three popular open-source intrusion detection systems, namely Snort, Suricata and Bro. Their experiments showed Bro provides better performance than other IDS systems due to the use of better classifier [30].

Comparing with all the works present in the literature the IDA proposed in this paper differs in many ways. First, most of the existing systems are developed for securing the networks. The existing systems such as a SNORT are network-based IDSs, on the other hand, the proposed system is a host-based IDS made for systems. However, the proposed systems uses KDD data set for effective evaluation. However,

the proposed system provides more than 98% of detection accuracy and hence, reduces the false positive rate. Finally, the main advantage of the proposed system is its accuracy in feature selection and classification.

3. Proposed System Architecture

The architecture of the system proposed in this paper consists of six major components, namely data set, Data Collector and Preprocessing module, Classification, Mapping module and modified KNN classifier as shown in the Figure 1.

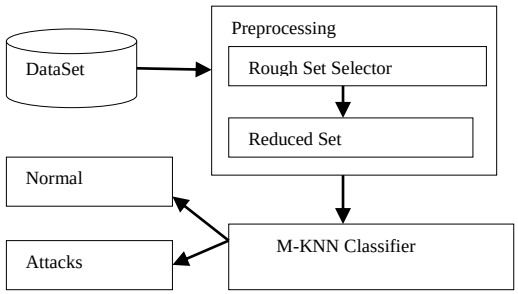

Figure 1. Intrusion detection system.

In this work, the KDD data set is used to carry out the experiments. This is a standard set of data which was audited, and includes a wide variety of intrusions simulated in this network environment, was provided. A connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows to and from a source IP address to a target IP address under some well-defined protocol. Each connection is labelled as either normal or as an attack, with exactly one specific attack type. Each connection record consists of about 100 bytes.

It is important to note that the test data is not from the same probability distribution as the training data, and it includes specific attack types not in the training data. This makes the task more realistic. Some intrusion experts believe that most novel attacks are variants of known attacks and the "signature" of known attacks can be sufficient to catch novel variants. The dataset contains a total of 24 training attack types, with an additional 14 types of the test data only. Table 1shows the different types of attack are present in the KDD dataset [13].

Table 1. Different types of attacks in KDD dataset.

Attack Classes	Attacks
Probing	ipsweep, nmap, portsweep, satan
Denial of Service (DOS)	back, land, neptune, pod, smurf, teardrop
User to Root (U2R)	buffer_overflow, perl, loadmodule, rootkit
Remote to User (R2L)	ftp_write,guess_passwd,imap,multihop,phf,spy, warezclient, warezmaster

In this proposed work, dimensionality is reduced using an MDMS feature selection algorithm and the attacks are detected under modified KNN classification.

- The proposed is the dimensionality reduction in fuzzy rough sets using Minimum Dependence Maximum Significance (MDMS) algorithm.
- MDMS algorithm calculates the dependency value and rank the goodness of the feature.
- Significant features are only considered and thereby attributes are reduced.

Feature Selection Algorithm is to select the best features from a huge data set so as to reduce the computational time. Since, among the huge number of attributes or features present in real-life data sets, only a small fraction of them are effective to represent the data set accurately. Our proposed work reduces the computational time for detecting the attacks. MDMS algorithm reduces the number of attributes by selecting only the significant attributes. The significance is ranked on the basis of dependency value. Maximum of dependency, higher the significance value and those attributes added to the significant features. The above steps are repeated until we the attributes are reduced to the significant values.

The performance analysis of this proposed work is done using the modified KNN Classifier. Modified KNN compares the training data set and testing data set and finally evaluates the performance of our reduced attributes with the real world data set. With the modified KNN classifier the computational time is reduced and thereby overlapping of classes can be avoided. Modified KNN compares the training data set and testing data set and finally evaluates the performance of our reduced attributes with the real world data set.

4. Extraction Feature Selection Algorithms

4.1. Feature Selection

This section explains the concept of feature selection, feature classification. Algorithm 1 describes the algorithm used for feature selection.

- *Step* 1: Calculate the equivalence classes for each conditional attributes and also for the decision attributes by Equation (1) [30].

$$IND(P) = \left\{(x_i, x_j) \in U \times U \forall a \in P, f(x_i, a) = f(x_j, a)\right\} \quad (1)$$

IND- indiscernibility, *U*-universal set, x_i ,x_j are the equivalence classes and *P*-subset in a data set. The indiscernibility relation is to calculate the equivalence classes. The equivalence classes are the classes that have the similar characteristic objects. Objects of the same rank can be grouped into a single class. Likewise the objects are classified under various equivalence classes.

Algorithm 1: Rough Set Based Feature Selection Algorithm

Input: Set of 41 features from KDD data set
Output: A reduced set of six attributes Si.
Step1 : Select the all attributes
D(A_1, A_2, ……,A_n) Data set, δ – threshold.
step2: For i = 1 to n do
Step3: Select and remove the redundant columns
Step4: End for
Step5: for i = 1 to n do
Step6: Calculate threshold δ
Step7: Fuzzy classes $\{\mu\overline{P}(F_i), \mu\underline{P}(F_i)\}$
Step8: Calculate dependency γ_c
Step9: End for
Step10: for F_i of max γ_c do
Step11: if(γ_c> δ) S_i =F_i
Step12: else if(γ_c=0) I_i= F_i
Step13: else if(γ_c> δ) D_i = F_i
Step14: end for
Step15: Return S

- *Step* 2: Remove the redundant attributes. Data set may contain useful as well as unwanted information that has no predictive measure. Removing those redundant or unwanted attributes may help us in reducing the computational time.
- *Step* 3: Using Equations (2) and (3) calculate the fuzzy Approximations to calculate the positive region of the attribute.

$$\mu\overline{P}(F_i) = \sup\{\mu F_i(x), \mu\overline{P}X(F_i)\} \quad (2)$$

$$\mu P\_(F_i) = \sup\{\mu F_i(x), \mu P\_X(F_i)\} \quad (3)$$

μ-membership function, F_i -Fuzzy equivalence class, sup -supremum, $\overline{P}$ -Fuzzy lower approximation, $P\_$ -Fuzzy upper approximation. Fuzzy lower and upper approximations are to calculate the positive region of the conditional attribute with respect to the decision attribute and then the dependency.

- *Step* 4: Calculate the positive region of the conditional attribute for decision attribute.

$POS = U\underline{C}X_i$, X_i is the *i*th equivalence class.

POS – Positive region of the attribute.

The positive region of the conditional attributes can be computed from the fuzzy lower approximation.

- *Step* 5: Calculate the dependency value with the calculated positive region of the attribute.

$$\gamma_c = \frac{|POS_c(D)|}{|U|} \quad (4)$$

γ_c– Dependency value of the attribute.

Dependency value is calculated to find the significance of the attributes. It shows the importance of the feature on predicting the result.

- *Step* 6: Categorize the dependent attributes of high value into the significant, insignificant and dispensable set. Significant set has the attributes of high dependent value. These are the most important attributes in predicting the result.

$$S_i = \{A_j \mid \sigma(A_j, D) > \delta_i\} \quad (5)$$

The insignificant set has the attributes that have zero level predictive measure. So this set is rejected or omitted.

$$I_i = \{A_j \mid \sigma(A_j, D) < -\delta_i\} \quad (6)$$

The dispensable set has the attributes that have either predictive or non-predictive measure. This has to be run in a loop for finding the dependent value and considered to a significant extent.

$$D_i = \{A_j \mid \sigma(A_j, D) \leq -\delta_i\} \quad (7)$$

Finally the attributes are reduced to the significant set. A_j-Conditional Attribute value, D-Decisions Attribute value, σ -Significance value and δ- Threshold value.

4.2. Modified K-NN Classifier

In this work, the Modified KNN Classifier [14] compares the test data set and train data set. In the data set, 70% is used for training and 30% for testing. It compares the performance ratio for both training and testing data set..

Algorithm 2: Modified KNN Algorithm
Input: F (f1, f2, ...fn) Selected Features
Output: Return Labelled Classes

1. *Set k, the number of neighbors*
2. *Calculating the Nearest Neighbors from F*
3. *Initialize E to NULL*
4. *For i=1 to n do begin*
5. *Calculate the Euclidean distance from node to member x_i*
6. *Compute the Fuzzy membership value*
7. *Apply fuzzy rule to check nearness.*
8. *If i < k then*
9. *Add member to set E*
10. *Else if i=k then*
11. *Assign member as the nearest neighbors.*
12. *Else*
13. *Delete the member from the set.*
14. *End for*
15. *Read c;*
16. *For i=1 to c*
17. *Calculate the membership* μ_i
18. *Add label to the vector.*
19. *End for*
20. *Return labeled classes*

The basis of the proposed modified KNN algorithm is to assign membership using Gaussian membership function as a function of the data values distance from its K-nearest neighbors and the memberships in the possible classes. This modified KNN algorithm assigns class membership to the given vector rather than assigning the vector to a particular class. The advantage is that no arbitrary assignments are made by the algorithm. In addition, the vector's membership

values provide improved classification accuracy. Algorithm 2 explains the steps of the proposed Modified KNN algorithm.

5. Analysis of Experimental Results

5.1. Calculating Reduced Feature Set

Using the positive regions, the dependencies (γ) of the attributes with respect to the decision attribute is calculated in this work. Finally, the attributes with the maximum dependency value are taken and considered for further calculation and this iteration continues until the minimum set of attributes are found out. Table 2 shows the dependency values of the attributes from the data set.

Table 2. Dependency values of the attribute.

Chosen Attributes	Dependency Value
Choosing {4}	0.6285
Choosing {4,22}	0.80425
Choosing {4,22,31}	0.965
Choosing {4,22,31,37}	0.965
Choosing [4,22,31,,36,37]	0.9975
Choosing {4,5,22,31,36,37}	1.0
The Selected Attributes are {4,5,22,31,36,37,41}	

The calculation denotes the values of the dependency that is based on the concept that the attribute with the maximum dependency is selected. Our Proposed work reduces the computational time for detecting the attacks. The proposed rough set based feature selection algorithm reduces the number of attributes by selecting only the significant attributes. Table 3 shows the names of the selected attributes.

Table 3. Name of the selected attributes.

S.No	Name of Selected Attributes
1	Dst_bytes
2	Flag
3	Count
4	Dst_host_count
5	Dst-host_srv_diff
6	Dst_host_srv_serror_rate

5.2. Performance of Modified Classifier

In this work, we have used the Modified- KNN for effective classification of the data set. Moreover, KNN is a non-parametric lazy learning algorithm and hence it does not make any assumptions on the underlying data distribution. Table 4 shows the detection rate provided by three classification algorithms, namely SVM, KNN and M-KNN.

Table 4. Detection rate with full set of features.

Exp. No.	SVM			KNN			M-KNN		
	Probe	DoS	Others	Probe	DoS	Others	Probe	DoS	Others
1	90.15	91.47	54.52	94.78	93.56	58.13	98.10	98.58	69.59
2	89.17	90.14	56.45	95.45	93.47	57.21	98.90	98.14	68.31
3	89.25	91.52	55.95	95.25	94.23	58.05	98.72	98.25	69.15
4	90.15	90.63	55.41	96.14	94.14	57.89	98.25	97.45	69.17
5	90.28	91.15	56.33	96.78	94.27	58.10	98.15	97.07	68.78

From Table 4, it is observed that the detection rate is high when M-KNN is applied for classification. This is due to the fact that Modified KNN uses fuzzy rules derived from Gaussian membership function which is used for decision making along with distance measurements. When it is compared with SVM, the performance of M-KNN is more significant. Similarly, the performance of KNN is not sufficient to reduce the false alarm rate. Table 5 shows the detection rate obtained from five experiments carried out with 10,000 records of the data set for each experiment on three classifiers namely SVM, KNN and M-KNN having the same percentage of training data set for all the three algorithms. Similarly, 30% of the data set were taken for performing the testing.

Table 5. Detection rate with reduced set of features.

Exp. No.	SVM			KNN			M-KNN		
	Probe	DoS	Others	Probe	DoS	Others	Probe	DoS	Others
1	92.13	93.30	60.73	96.20	96.00	63.47	99.51	99.29	71.62
2	91.78	92.15	61.10	97.55	96.24	65.05	99.25	99.45	69.42
3	92.67	93.20	60.92	97.25	96.25	64.60	99.14	99.75	74.32
4	92.29	93.18	61.20	98.30	95.98	64.72	99.13	99.23	73.43
5	92.23	93.90	62.43	98.50	96.89	63.20	99.18	99.24	71.17

From Table 5 it is observed that the detection rate is increased when selected features are used. This is due to the fact that the fuzzy rules applied on reducing features set have equivalent crisp set rules. Moreover, they are no contradicting attributes which made the decision process easier for all the three algorithms, namely SVM, KNN and M-KNN.

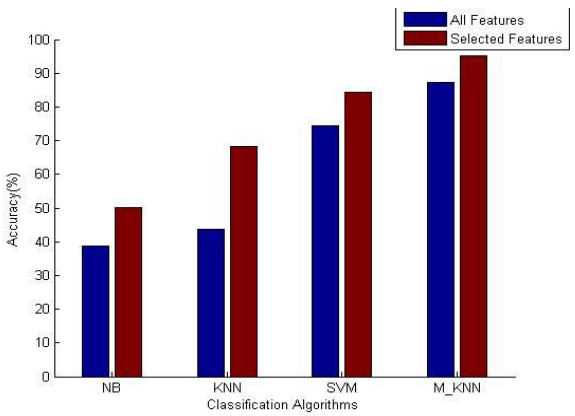

Figure 2. Accuracy analysis for classifiers.

Figure 2 shows the accuracy analysis for the four classifiers namely Naïve Bayes classifier, SVM, KNN

and Modified KNN. From this figure, two observations can be made. First, the selected set of features increases the classification accuracy. This is due to the fact that selected features take only the necessary rules for decision making. Therefore, the classifier is not confused, leading to increasing in accuracy. Second, Modified KNN outperforms all the other algorithms. This is because Modified rules are overcoming the boundaries in decision making.

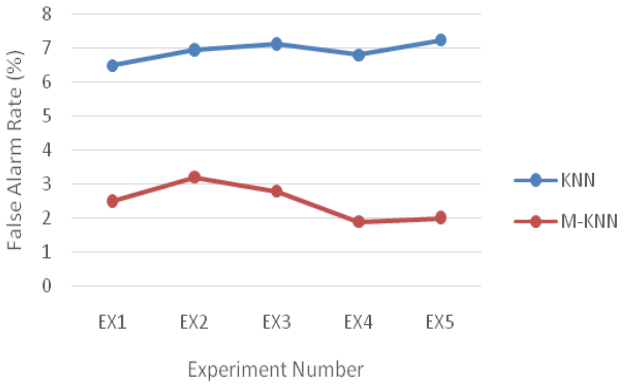

Figure 3. False alarm rate analysis.

Figure 3 shows the false alarm rate analysis for the two classifiers namely KNN and Modified KNN. From Figure 3 it is observed that modified KNN has less false alarm rate in comparison with KNN. This is because; in all the five experiments fuzzy rules were applied for conflict resolution.

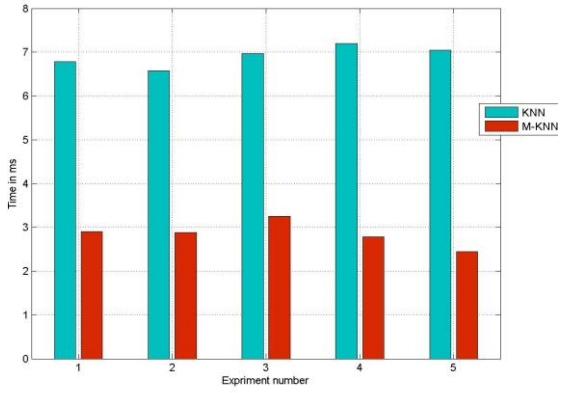

Figure 4. Time analysis.

Figure 4 shows the time analysis for the two classifiers namely KNN and modified KNN. From Figure 4 it is observed that modified KNN takes less time in comparison with KNN. This is because in all the five experiments fuzzy rules were applied for fast convergence.

6. Conclusions

In this proposed work, a new IDS has been developed and implemented with a simple feature selection algorithm. The work was carried out on selected attributes computing the result with 41 attributes seems to be very complicated and difficult to achieve accuracy. The proposed work selects only the significant features that have the highest probability of predictive measure. With the reduced set, we have reduced the computation time. Further, the Modified K-NN classifier helped in achieving the greater the accuracy. Hence, we computed the result in an efficient manner to prevent the attacks that improve the security.

References

[1] Bi J., Bennett K., Embrechts M., Breneman C., and Song M., "Dimensionality Reduction Via Sparse Support Vector Machines," *Journal of Machine Learning Research*, vol. 3, pp.1229-1243, 2003.

[2] Debar H., Me L., and Wu S., "Recent Advances in Intrusion Detection," *in Proceedings of the 3rd International Workshop*, Toulouse, pp. 53, 2000.

[3] Debar H., Becker M., and Siboni D., "A Neural Network Component for an Intrusion Detection System," *in Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, pp. 240-250, 2012.

[4] Dy J., and Brodley C., "Feature Selection for Unsupervised Learning," *The Journal of Machine Learning Research Archive*, vol. 5, pp. 845-889, 2004.

[5] Eesa A., Orman Z., and Brifcani A., "A Novel Feature-Selection Approach Based on the Cuttlefish Optimization Algorithm for Intrusion Detection Systems," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2670-2679, 2015.

[6] Forman G., "An Extensive Empirical Study of Feature Selection Metrics for Text Classification," *Journal of Machine Learning Research*, vol. 3, pp. 1289-1305, 2003.

[7] Fossaceca J., Mazzuchi T., and Sarkani S., "MARK- ELM:Application of A Novel Multiple Kernel Learning Framework for Improving the Robustness of Network Intrusion Detection," *Expert Systems with Applications*, vol. 42, no. 8, pp. 4062-4080, 2015.

[8] Ganapathy S., Vijayakumar P., Palanichamy Y., and Arputharaj K., "An Intelligent CRF Based Feature Selection for Effective Intrusion Detection," *The International Arab Journal of Information Technology*, vol. 13, no. 1, pp. 44-50, 2016.

[9] Gondaliya T. and Singh M., "Intrusion Detection System for Attack Prevention in Mobile Ad-Hoc Network," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 4, pp. 638-641, 2013.

[10] Hoque M., Abdul-Mukit M., and Abu-NaserBikas M., "An Implementation of Intrusion

Detection System Using Genetic Algorithm," *International Journal of Network Security and its Applications*, vol. 4, no. 2, pp. 109-120, 2012.

[11] Jensena R., Tusonb A., and Shena Q., "Finding Rough and Fuzzy-Rough Set Reduces with SAT," *Information Sciences*, vol. 255, pp. 100-120, 2014.

[12] Kartit A., Saidi A., Bezzazi F., Marraki M., and Radi A., "A New Approach to Intrusion Detection System," *Journal of Theoretical and Applied Information Technology*, vol. 36, no. 2, pp. 284-289, 2012.

[13] KDD Cup 1999 Intrusion Detection Data available at: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, Last Visited, 2010.

[14] Law K. and Kwok L., "IDS False Alarm Filtering Using KNN Classifier," *in Proccedings of 5th International Workshop on Information Security Applications*, Jeju Island, pp. 114-121, 2005.

[15] Maji P. and Garai P., "IT2 Fuzzy-Rough Sets and Max Relevance-Max Significance Criterion for Attribute Selection," *IEEE Transactions on Cybernetics*, vol. 45, no. 8, pp. 1657-1668, 2015.

[16] Moradi M. and Zulkernine M., "A Neural Network based System for Intrusion Detection and Classification of Attacks," *in Proceedings of IEEE International Conference on Advances in Intelligent Systems-Theory and Applications*, pp. 15-18, 2011.

[17] Mulay S., Devale P., and Garje G., "Intrusion Detection System using Support Vector Machine and Decision Tree," *International Journal of Computer Applications*, vol. 3, no. 3, pp. 975-987, 2010.

[18] Nader P., Honeine P., and Beauseroy., "Normsin One-Class Classificationfor Intrusion Detectionin SCADA Systems," *Industrial Informatics, IEEE Transactions*, vol. 10, no. 4, pp. 2308-2317, 2014.

[19] Onut I. and Ghorbani A., "A Feature Classification Scheme for Network Intrusion Detection," *International Journal of Network Security*, vol. 5, no. 1, pp. 1-15, 2007.

[20] Patel A., Taghavi M., Bakhtiya K., and Junior J., "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 25-41, 2013.

[21] Qassim Q., Patel A., and Mohd-Zin A., "Strategy to Reduce False Alarms in Intrusion Detection and Prevention Systems," *The International Arab Journal of Information Technology*, vol. 11, no. 5, pp. 500-506, 2014.

[22] Rajeswari L. and Arputharaj K., "An Active Rule Approach for Network Intrusion Detection with Enhanced C4.5 Algorithm," *International Journal of Communications, Network and System Sciences*, vol. 4, pp. 285-385, 2008.

[23] Ramaswami M. and Bhaskaran R., "A Study on Feature Selection Techniques in Educational Data Mining," *Journal of Computing*, vol. 1, no. 1, pp. 7-11, 2009.

[24] Sarasamma S., Zhu Q., and Huff J., "Hierarchical Kohonen Net for Anomaly Detection in Network Security," *IEEE Transactions on System, Man, Cybernetics, Part Cybernetics*, vol. 35, no. 2, pp. 302-312, 2005.

[25] Sathya S., Ramani R., and Sivaselvi K., "Discriminant Analysis based Feature Selection in KDD Intrusion Dataset," *International Journal of Computer Application*, vol. 31, no. 11, pp. 1-7, 2011.

[26] Senthilnayaki B., Venkatalakshmi K., and Kannan A., "An Intelligent Intrusion Detection using Genetic based Feature Selection and Modified J48 Decision Tree Classifier," *in Proccedings of 5th International Conference on Advanced Computing*, Chennai, pp. 1-7, 2013.

[27] Senthilnayaki B., Venkatalakshmi K., and Arputharaj K., "Intrusion Detection System Using Feature Selection and Classification Technique," *International Journal of Computer Science and Application*, vol. 3, no. 4, pp. 145-151, 2014.

[28] Shittu R., Healing A., Ghanea-Hercock R., Bloomfield R., and Rajarajan M., "Intrusion Alert Prioritisation And Attack Detection Using Post-Correlation Analysis," *Computers and Security*, vol. 50, pp. 1-15, 2015.

[29] Sindhu S., Subbiah G., and Arputharaj K., "Decision Boundary based Light Weight Intrusion Detection using a Wrapper Approach," *Expert Systems with Applications*, vol. 39, no. 1, pp. 129-141, 2012.

[30] Thongkanchorn K., Ngamsuriyaroj S., and Visoottiviseth V., "Evaluation Studies of Three Intrusion Detection Systems under Various Attacks and Rule Sets," *in Proceedings of IEEE International Conference of IEEE Region 10 (TENCON)*, Xi'an, pp. 1-4, 2013.

Balakrishnan Senthilnayaki has completed MTech and PhD at (CEG) Anna University, Chennai-25. She has 7 years of teaching experience. Currently, she is working as a Teaching Fellow of the (CEG) Anna University, Chennai. She has 12 publications in journals and conference proceedings. Her areas of interest include Data Mining, DBMS and Soft Computing.

Krishnan Venkatalakshmi has completed ME and PhD at Thigarajar Engineering College, Madurai. She has 15 years of teaching experience.Currently, She is head and Assistant Professor in the Department of Electronics and Communication Engineering at Anna University (UCET) Tindivanam. She has more than 53 publications in reputed journals and conference proceedings. Her area of interest includes Signal Processing, VLSI, Wireless Networks, Wireless Communication and Instrumentation.

Arputharaj Kannan has completed ME and PhD at Anna University, Chennai-25. He has 25 years of teaching experience at Anna University. Currently, he is Professor and Head of the Department of Information Science and Technology at Anna University, Chennai. He has more than 225 publications in reputed journals and conference proceedings. His areas of interests include DBMS, Data Mining, Artificial Intelligent and Software Engineering.