Journal of Intelligent & Fuzzy Systems 34 (2018) 1243–1250
DOI:10.3233/JIFS-169421
IOS Press

A novel intrusion detection system for wireless mesh network with hybrid feature selection technique based on GA and MI

R. Vijayanand[a,*], D. Devaraj[b] and B. Kannapiran[c]
[a]*Department of Computer Science and Engineering, Kalasalingam University, Tamilnadu, India*
[b]*Department of Electrical and Electronics Engineering, Kalasalingam University, Tamilnadu, India*
[c]*Department of Electronics and Instrumentation Engineering, Kalasalingam University, Tamilnadu, India*

Abstract. Intrusion detection is an important requirement in wireless mesh network and the intrusion detection system (IDS) provides security by monitoring data traffic in real time. This work proposes support vector machine (SVM) classifier to identify the intrusion in the network. The traffic data collected from the wireless mesh network (WMN) is given as input to the SVM. The irrelevant and redundant input variables increase the complexity of designing IDS and may degrade its performance. Hence, feature selection techniques, which select the relevant features from the original input is essential to improve the performance of IDS in WMN. In this work, a hybrid genetic algorithm (GA) and mutual information (MI) based feature selection technique is proposed for IDS. The performance of IDS with the proposed feature selection technique is analyzed with IDS having mutual information, genetic algorithm and GA+MI based feature selection techniques using ADFA-LD dataset. Experimental results have demonstrated the effectiveness of proposed intrusion detection system with hybrid feature selection technique in wireless mesh network. The superiority of SVM classifier with hybrid feature selection technique is also verified by comparing with artificial neural network classifier.

Keywords: IDS for WMN, SVM based IDS, ADFA-LD dataset, GA with MI technique, Hybrid feature selection

1. Introduction

The high speed data transmissions and cost-effectiveness have made the wireless mesh network as a suitable technology for various applications like smart grid, Internet of Things (IoT), etc [1]. The multi-hop nature of WMN increases the probability of attacks like denial of service, selective forwarding, worm-hole, sink-hole, black-hole, etc in the network. Intrusion detection system provides security against these attacks effectively. In WMN, intrusion detection algorithms are implemented in different fashions such as optimized monitoring functions [2], energy efficient monitoring [3], firewall [4], etc. Most of the available intrusion detection system (IDS) falls under the third category in which intrusions are detected by classifying traffic data into normal and attack data [5]. In some cases, combinations of optimal monitoring of traffic and energy level of node simultaneously have been applied as in [6]. Some of the traffic aware IDS like FADE [7] detects grey-hole attacks using the acknowledgement information of transmitted packets. However, the accurate traffic knowledge may not be available in most of the networks. In that case, a traffic agnostic based approach

[*]Corresponding author. R. Vijayanand, Department of Computer Science and Engineering, Kalasalingam University, Tamilnadu, India. E-mail: rkvijayanand@gmail.com.

1064-1246/18/$35.00

like RAPID [8] is used to detect intrusions. It uses the link coverage knowledge of WMN to analyze traffic in centralized and distributed fashion.

Machine learning algorithms like learning automata [9], SVM [10], etc are used to detect intrusions by learning the traffic flow information of WMN. The major issue in the implementation of machine learning technique based IDS in WMN is dimensionality problem. The requirement of large amount of energy to deal with the dimensionality affects the efficiency of IDS in WMN. Another major drawback in the implementation of IDS with large number of features is the requirement of large execution time [11]. Hence, the large numbers of irrelevant features have to be removed from the traffic data for getting better detection accuracy.

Dimensionality reduction technique provides solution to that problem by identifying informative features and giving it as input to IDS. Feature extraction and feature selection are the two types of dimensionality reduction techniques. In feature extraction, the input variables are transformed into derived values which can be used for intrusion detection purpose [12]. It can be sub classified as linear methods like independent component analysis [13], partial least squares [14], principal component analyses [15], etc and non-linear methods like ensemble localized manifold [16], etc based on the implementation mechanism. In most of the real world applications, the features generated by feature extraction technique have no clear physical meaning and are very hard to interpret by classifier [17].

Feature selection technique is simple and easy to implement compared to the former technique. It is defined as the selection of 'M' optimal subset of features from the original feature set for increasing the performance of machine learning models [18]. It is generally classified as filter and wrapper method. Filter method select the subset of features by evaluating the mutual relationship between features during output prediction, whereas, wrapper method uses predictive models to select the optimal subset of features.

Mutual Information is one of the widely used filter method based feature selection technique. It selects the informative features based on the relations between the features with corresponding output. It has difficulty during implementation in some real world applications, so an equivalent form, Minimum redundancy maximum relevancy (mRmR) is used to implement MI. In [19], mRmR based feature selection technique is proposed to select the informative features without considering the properties of individual class. Several other methods like sparse kernel [20], SVM weight vector [21], etc are proposed to select the optimal features from the dataset. Most of the feature selection methods belong to the category of wrapper method in which classifiers like random forest [22], SVM [23], etc are used to select the optimized subset of features.

Recently, evolutionary techniques like GA and particle swarm optimization [24] have been applied to select the most informative features from the original features. Both filter and wrapper methods have merits and demerits and it is desirable to embed both wrapper and filter approach to get an effective feature selection algorithm. In the proposed work, a novel IDS is designed for WMN using a hybrid feature selection technique based on genetic algorithm and mutual information.

2. Intrusion detection in wireless mesh network

Intrusion detection is the process of identifying the occurrence of different attacks in a network by analyzing the features of network traffic for providing security to a network. WMN has advanced routing protocols for providing guaranteed communication with end devices. The attacks on routing protocols could damage the entire communication network. Thus the routing based impersonation attacks like black hole, grey hole, etc are frequently used by attackers against WMN. Traffic based IDS efficiently detects these attacks by analyzing the traffic data and routing information.

The IDS in WMN is categorized into cooperative IDS, monitored IDS and traffic aware IDS. In cooperative IDS, each node has some functions to detect intrusions and the detected information is shared periodically [25]. This mechanism requires limited energy compared to other approaches but also has low accuracy rate in the changing dynamic environment. In the monitored IDS, a small group of nodes are selected for monitoring the suspicious part of the network [26]. Large numbers of nodes are required to monitor some of the attacks like selective forwarding attack. Recently, traffic aware IDS gets much importance that monitors the entire communication links by placing IDS on WMN nodes along the routing path instead of IDS at particular nodes. The traffic aware IDS has good accuracy in attack detection because individual nodes monitor the network traffic based on traffic pattern.

The lack of single vantage point and limited resources of nodes requires an advanced intrusion detection system for monitoring the network traffic in WMN. The classifiers like SVM, ANN, etc support the IDS in the classification of traffic data as normal and attack data. The IDS are classified as anomaly and misuse based detection technique based on classifier training with normal and attack data respectively. Node failures and variation in link quality by noisy environment are some of the factors affecting the detection accuracy of intrusion detection system [27]. Sometimes missing and inclusion of some irrelevant features also affect the classification accuracy of traffic based IDS in a resource constraint WMN. The selection of informative features has various advantages like reducing false positive rate, cost effectiveness and energy conservation of WMN. Hence in the proposed work, the feature selection technique is applied to identify the relevant features, and the selected features are given to the IDS.

3. Proposed technique for intrusion detection

In WMN, attacks are of different types and multi attack detection classifier is required in most cases. SVM classifier can accurately detect multiple attacks and is suitable for WMN IDS [28]. The development of SVM has two stages, training and testing. The collected data is divided into training and testing data. Training data is used to train the SVM and the test data is used to evaluate the performance of the trained SVM.

Figure 1 shows the block diagram representation of the training stage of the SVM based IDS. Classifiers have low accuracy rate due to redundant and irrelevant features generated by the applications. Hence, feature selection techniques are necessary for selecting the informative features for accurate detection of attacks. In this work, the informative features are selected using hybrid GA and MI based feature selection technique and are used to train the SVM classifier. Feature selection techniques acts as a backbone for this kind of application because most of the features look like similar and some features affect the performance of classifier.

The SVM classifier is trained with the optimal subset of features selected using hybrid GA and MI technique and is evaluated with testing data before being implemented in real environment. The details of the SVM classifier and feature selection technique are presented in the subsequent sections.

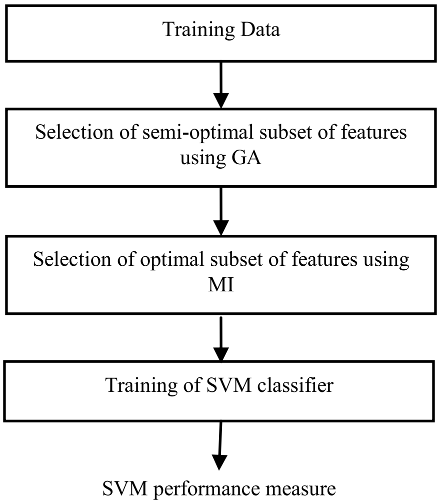
Training Data
Selection of semi-optimal subset of features using GA
Selection of optimal subset of features using MI
Training of SVM classifier
SVM performance measure

Fig. 1. Training stage of the SVM based IDS.

4. SVM classifier

SVM classifier is a supervised learning algorithm based classifier that is designed with the basic idea of separating class with a straight line given by the Equation (1),

$$f(x) = W^T X + b = 0 \tag{1}$$

where W is weight vector and b is bias. In complex datasets, classification is performed by curve instead of line. Thus for achieving the classification in complex dataset, the input data is initially mapped into feature space and is linearly separated by a separable hyperplane [29].

The mapping operation is carried out by 'kernel' function and choosing different kernel functions will produce different convergence rate. Linear, Quadratic, Polynomial, Multilayer Perceptron (MLP) and Gaussian are some of the widely used kernel functions in SVM classifier. The linear kernel function has low accuracy in the classification of complex datasets where some data cannot be separated linearly. So, the other kernel functions are used in most cases. The architecture of SVM is shown in Fig. 2, where X is the input data having 'n' number of features and is given to 'm' kernel functions. In this work, MLP kernel function [30] is used to map the input data into kernel space for finding the maximum margin hyperplane. The MLP kernel function of SVM has number of hidden layers that focus on the minimization of error functions with the help of support vector coefficient 'k' and bias value 'θ'. The kernel function maps the input data into the default scale value of

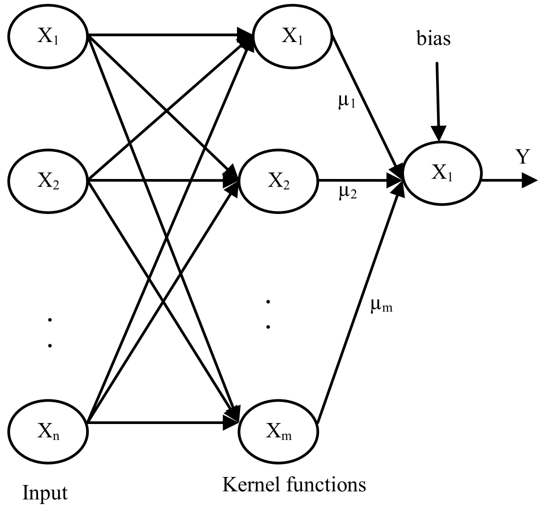

Fig. 2. SVM Architecture.

[+1, –1]. The training of hidden layers for the input data X_i is represented in Equation (2),

$$K_m = \tanh\left(kx_i^T x + \theta\right) \tag{2}$$

The minimization of error tunes the hidden layer margin which is reflected in maximal margin of hyperplane. The training is repeated till each output data are correctly matched. In general, the separable line with global margin (2/||w||) is selected by most of the classifiers for classifying data with maximum accuracy [31].

SVM classifier is generally designed from known labeled training data and its accuracy is analyzed using testing data. The Multiclass SVM is proved to be as accurate in the classification of multiple classes than any other technique. The number of classifiers used in Multiclass SVM depends on the number of classes in the dataset. In this model each classifier is trained by the dataset with consideration of classifier's corresponding class as '1' and all other classes as '0'. The classifier trained with such kind of classification dataset produces high accuracy. The individual classifier output is noted for all dataset and the final prediction is based on the confidence value for each class. Mathematically it is represented as,

$$\text{class} = \arg \max_{i=1...n} \text{ of } g_i$$

where n represent the number of classes, g_i is the individual value of ith classifier and class is the output of high confidence value classifier. Once the classifier is trained and tested, they are ready to classify the data in real environment.

SVM classifier has good capability on dealing with nonlinear data that makes it as most suitable for intrusion detection systems [32]. SVM based IDS has excellent performance by implementing in various orders like distributed [26, 32], hierarchical [33], etc. The usage of SVM in IDS requires extensive memory because of large dimensionality in network datasets and also affects the accurate detection ratio.

5. Hybrid feature selection techniques

The non relevant and redundant features decrease the accuracy of intrusion detection classifier along with increasing time and space complexity. Thus the selection of optimal features is essential to detect intrusions efficiently. A novel hybrid GA and MI based feature selection technique is used in this work to reduce the dimensionality and select the optimal subset of features for an intrusion detection system as shown in Fig. 3.

In this paper, the proposed IDS with feature selection technique uses accuracy rate of classifier as the objective. In the proposed feature selection technique, Genetic algorithm [34] initially generates the random chromosome of population from original features of the data and selects the semi informative features. Once the semi informative features are selected, the fitness level of each chromosome for that generation

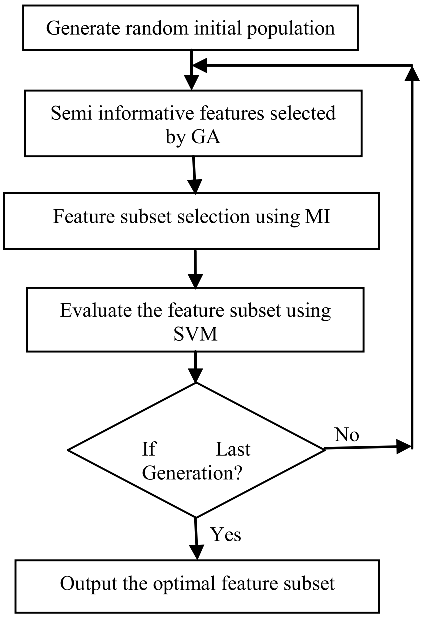
Generate random initial population
Semi informative features selected by GA
Feature subset selection using MI
Evaluate the feature subset using SVM
If Last Generation?
No
Yes
Output the optimal feature subset

Fig. 3. Proposed feature selection technique.

is calculated with the help of Mutual Information (MI) technique [35] and SVM classifier. The features are given as input to MI which selects features with high mutual information value from the individuals in the selected population. The mutual information is calculated as follows:

$$h_y = -\sum_{j=1}^{N_y} P\left(Y_j\right).log\left(P\left(Y_i\right)\right) \tag{3}$$

Where h_y is entropy, N_y is number of classes included in the training data and $P(y_j)$ is the probability of individual class.

$$h_{(y/x)} = -\sum_{i=1}^{N_x} P\left(X_i\right) \sum_{j=-1}^{N_y} P_{YX} \tag{4}$$

Where $P_{YX} = P(Y_j/X_i).\log P(Y_j/X_i)$, $h_{(y/x)}$ is conditional entropy value, N_x is number of input variable and $P(Y_j/X_i)$ is the probability of individual input value to the corresponding output and $P(X_i)$ is the probability of possible values in the input features.

$$I\left(Y : X\right) = h_y - h_{(y/x)} \tag{5}$$

Finally the mutual information value I(Y;X) of each feature is calculated by Equation (5). The features with high mutual information value will have high impact on intrusion detection that is marked as informative features. If an application has large number of features with low mutual information value those features will not have major impact on the accuracy of classifier and can be removed as non informative features.

The implementation mechanisms generally followed in the MI selection process is by selecting the features with high mutual information value as informative features. In this work, the top 'm' number of informative features is going to be selected by the proposed technique from a network data. The selected features are given as input to SVM classifier for the classification of normal and attack data. The accuracy of the classifier is used to evaluate the individuals in the population. After the fitness of all individuals is evaluated, the top chromosomes in the population are selected as parent chromosomes for next generation for further optimization process. In this work, tournament based selection technique is used to select the most optimal solutions from the population. After selecting the parent chromosomes for next generation, they will undergo crossover and mutation operations. In crossover operation, some blocks of the chromosomes are randomly swapped and in the mutation operation some bits of chromosomes are shifted from 1 to 0 or 0 to 1 based on the crossover and mutation rate respectively. The crossover operator helps to generate the new offspring for each generation whereas the mutation operator helps to avoid the problem from stucking at local minima. This process is repeated till the specified number of generations is reached.

The proposed hybrid feature selection technique combines the merits of both wrapper and filter method based feature selection techniques. The main features of the proposed method are,

1. The usage of filter method based on mutual information helps to avoid the trapping of Generic algorithm based wrapper method at local minima.
2. A good subset of features reduces the computational effort of training the classifier by removing less informative features. In the proposed hybrid technique, the most informative features are only selected because MI selects the features from the optimal features selected by GA.
3. The optimal features selected by the proposed technique increase the correct classification ratio by reducing the error rate of classifier.

6. Experimental results

This section presents the details of the development of SVM-based IDS using ADFA-LD dataset. Most of the attacks in wireless mesh network are similar to this dataset and is most suitable to analyze the IDS of wireless mesh network with this dataset. The ADFA-LD dataset has 49 features to represent 9 attacks and a normal class data. But in this experiment, the dataset are reduced to 6 attacks and 1 normal class by combining similar category of attacks.

In this experiment, informative features of ADFA-LD intrusion dataset [36] are acquired with the help of proposed GA and MI based feature selection technique. Training and testing sets are randomly selected from ADFA-LD dataset and all the features are needed to be preprocessed before experimentation. The experiment has training data of size 300 dataset (41 normal, 73 Exploits, 7 DoS, 72 Fuzzers, 4 Backdoor, 102 Generic and 1 worm) over the testing data of 4002 dataset (1591 normal, 261 Exploits, 39 DoS, 313 Fuzzers, 4 Backdoor, 1792 Generic and 2 worms) are randomly selected to reduce the training time.

The experiment is carried out using Matlab in which the training and testing set are loaded in separate file. Initially after preprocessing the random population of chromosome is generated from the data of training set, the semi informative features are selected using genetic algorithm. The parameters of the GA are taken as population size: 20, generation: 10, mutation rate: 0.01 and crossover rate as 0.9. Then the random population of chromosome with selected features is given as input to mutual information technique for getting the compact most informative features. Then the compact informative features are given as input to SVM classifiers and the accuracy rate of classifiers is computed.

Based on the accuracy rate of classifiers as fitness level, the candidates feature used for next generation is further optimized by genetic algorithm. The chromosomes with large fitness value are selected as new parent for next generation and the process repeats till last generation. The optimal feature subset found by the hybrid feature selection technique is used to achieve maximum accuracy of classifier. The comparison of proposed technique based on detection ratio over other feature selection technique is shown in Table 1. Each column has filter based MI features, wrapper based GA features and GA+MI technique are used for comparison with proposed feature selection technique. The results clearly demonstrate the usage of feature selection techniques has high accuracy in attack detection than using with original features. The proposed feature selection technique with SVM and ANN classifiers on the basis of accuracy rate and training time are given in Fig. 4 and Table 2 respectively. In most of the cases, SVM classifier outperforms ANN classifier in all kinds of feature selection methods. It also indicates increasing the number of features does not increase the accuracy of classifier. The accuracy rate of hybrid feature selection has high accuracy over normal GA technique by using SVM classifier. Intrusion detection system requires large time for training with data because of classifier optimization and offline processing whereas the testing data does not require much time even for testing huge number of data [15]. Hence, in this paper training time gets much importance than testing time.

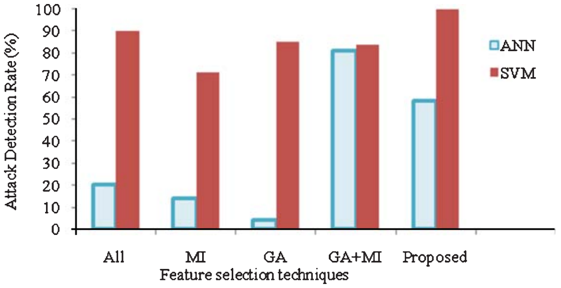

Fig. 4. Performance analysis of proposed IDS over ANN classifier.

Table 2
Comparison of SVM and ANN classifier based on training time (in second)

Techniques	No. of Informative Features	ANN	SVM
MI	5	21.52	12.91
GA	5	2813	117.86
GA+MI	5	3313	114.5
Hybrid GA & MI	3	2907	110.91

Table 2 verifies the proposed system has less training time than IDS with GA, MI and GA+MI techniques in both ANN and SVM classifiers. The proposed system is further validated by other standard datasets or cross validation of the dataset [37] or datasets generated as in [38] is essential to verify the performance in unseen data. In this work, widely used standard KDD cup ’99 dataset is used for validation and the results are given in Table 3. Thus from the results, the proposed IDS with hybrid feature selection technique detect the intrusions with high accuracy is verified. The selected optimal features reduce the computational effort of classifier and take less training time compared to the various available techniques. Eventhough the accuracy of classifier is improved by the proposed hybrid technique, the

Table 1
Comparison of proposed IDS with hybrid feature selection over other feature selection techniques

Techniques	Accuracy	Error rate	Sensitivity	Specificity	Precision
MI	0.7485	25.15	0.9284	0.2446	0.8652
GA	0.8582	0.1418	0.8575	0.8154	0.9868
GA+MI	0.9451	0.0549	0.9520	0.7990	0.9882
Hybrid GA & MI	1.0	0	1.0	1.0	1.0

Table 3
Validation of proposed system using KDD cup’99 dataset

Number of training data = 400			Number of testing data = 4565		
Technique	Accuracy	Error rate	Sensitivity	Specificity	Precision
MI	0.9616	0.384	0.9259	0.9781	0.9941
GA	0.9901	0.0099	1.0	0.9901	0.9904
GA+MI	0.9978	0.0022	0.9991	0.9842	0.9651
Hybrid GA & MI	1.0	0	1.0	1.0	1.0

training time of the classifier need to be further reduced for WMN based sensitive applications like smart grid, IoT, etc.

7. Conclusion

The usage of optimal features in the classification task is essential for designing good intrusion detection system in wireless mesh network. In this paper, a novel intrusion detection system with hybrid feature selection technique using genetic algorithm and mutual information technique is proposed. The wrapper method based genetic algorithm select the semi-optimal feature subset from the original subset. Then the mutual information technique placed inside the genetic algorithm selects the optimal feature subset with the help of SVM classifier and the process repeats till the maximum accuracy of IDS is achieved. The proposed IDS with hybrid feature selection technique is compared with the IDS using features selected by mutual information, genetic algorithm and GA+MI technique in SVM and ANN classifier. Experimental results have shown that the proposed intrusion detection system with hybrid GA and MI based technique with SVM classifier has high accuracy and can be suitable for intrusion detection system in wireless mesh network and other applications.

References

[1] S. Scott, Selfish insider attacks in IEEE 802.11s wireless mesh networks, *IEEE Communication Magazine* (2014), 227–233.

[2] H. Nguyen, G. Scalosub and R. Zheng, On quality of monitoring for multichannel wireless infrastructure networks, *IEEE Transactions on Mobile Computing* **13** (2014), 664–677.

[3] A. Hassanzadeh, R. Stoleru and B. Shihada, Energy efficient monitoring for intrusion detection in battery-powered wireless mesh network, In: *Proceedings of the ADHOC-NOW Workshop* (2011), pp. 44–57.

[4] X. Wang and P. Yi, Security framework for wireless communications in smart distribution grid, *IEEE Transactions on Smart Grid* **2** (2010), 809–818.

[5] B. Yang, L. Peng, Y. Chen, H. Liu and R. Yuan, A DGC-based data classification method used for abnormal network intrusion detection, *Lecture Notes on Computer Science* **4234** (2006), 209–216.

[6] O.E. Muogilim, K. Loo and R. Comley, Wireless mesh network security: A traffic engineering management approach, *Journal of Network and Computer Applications* **34** (2011), 478–491.

[7] Q. Liu, J. Yin, V.C.M. Leung and Z. Cai, FADE: Forwarding assessment based detection of collaborative grey hole attacks in WMNs, *IEEE Transactions on Wireless Communications* **12** (2013), 5124–5137.

[8] A. Hassanzadeh, R. Stoleru, M. Polychronakis and G. Xie, RAPID: Traffic agnostic intrusion detection for resource constrained wireless mesh networks, *Computer Security* **46** (2014), 1–17.

[9] S. Misra, P. Venkata Krishna, I. Abraham, N. Sasikumar and S. Fredun, An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks, *Computers & Mathematics with Applications* **60** (2014), 294–306.

[10] Y. Zhang, L. Wang, W. Sun, R. Green II and M. Alam, Distributed intrusion detection system in a multi-layer network architecture of smart grids, *IEEE Transactions on Smart Grid* **2** (2011), 796–808.

[11] R.O. Duda, P.E. Hart and D.G. Stork, Pattern classification, second ed. John Wiley and Sons Inc., USA (2000).

[12] B. Li, P. Zhang, H. Tian, S. Mi, D. Liu and R. Guo-quan, A new feature extraction and selection scheme for hybrid fault diagnosis of gearbox, *Expert systems with Applications* **38** (2011), 10000–10009.

[13] M. Kotani and S. Ozawa, Feature extraction using independent component analysis of each category, *Neural Processing Letters* **22** (2005), 113–124.

[14] C. Dhanjal, S.R. Gunn and J. Shawe-taylor, Efficient space kernel feature extraction based on partial least squares, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **31** (2016), 1347–1361.

[15] X. Gan, J. Duanmu, J. Wang and W. Cong, Anomaly intrusion detection based on PLS feature extraction and core vector machine, *Knowledge Based Systems* **40** (2013), 1–6.

[16] F. Li, L. Xu, A. Wong and D.A. Clause, Feature extraction for hyber spectral imagery via ensemble localized manifold learning, *IEEE Transactions on Geoscience and Remote Sensing* **12** (2015), 2486–2490.

[17] P. Ganesh Kumar and T. Aruldoss Albert Victoria, Multistage mutual information for informative gene selection, *Journal of Biological Systems* **19** (2011), 1–22.

[18] M. Dash, H. Liu and H. Motoda, Consistency based feature selection, *Lecture Notes on Computer Science* **1805** (2003), 98–109.

[19] H. Peng, F. Long and B.R. Moon, Feature selection based on mutual information: Criteria of max-dependancy, max-relevancy and min-redundancy, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **27** (2005), 1226–1238.

[20] P. Gurram and H. Kwon, Optimal kernel sparse learning in the empirical kernel space for hyberspace classification, *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing* **7** (2014), 1217–1226.

[21] E.E. Bron, M. Smits, W.J. Niessen and S. Klien, Feature selection based on the SVM weight vector for classification of Dementia, *IEEE Journal of Biomedical and Health Informatics* **19** (2015), 1617–1626.

[22] M. Pedergnana, P.R. Marpu, M.D. Mura, J.A. Benediktsson and L. Bruzzone, A novel technique for optimal feature selection in attribute profiles based on genetic algorithms, *IEEE Transactions on Geoscience and Remote Sensing* **51** (2003), 3514–3528.

[23] M.A. Ambusaidi, X. He, Z. Tan, P. Nanda, L.F. Tu and U.T. Nagar, A novel feature selection approach for intrusion detection data classification, In: *International conference on Trust, security and privacy in computing and communications* (2014), 82–89.

[24] P. Ghamisi and J.A. Benediktsson, Feature selection based on hybridization of genetic algorithm and particle swarm optimization, *IEEE Transactions on Geoscience and Remote Sensing* **12** (2015), 309–313.

[25] M. Saxena, M. Denko and D. Banerji, A hierarchical architecture for detecting selfish behaviour in community wireless mesh networks, *Computer Communications* **34** (2011), 548–555.

[26] D. Subhadrabandhu, S. Sarkar and F. Anjum, A framework for misuse detection in ad hoc networks-part I, *IEEE Journal on Selected Areas in Communications* **24** (2006), 274–289.

[27] A. Morais and A. Cavalli, A distributed and collaborative intrusion detection architecture for wireless mesh network, *Mobile Networks and Applications* **19** (2014), 101–120.

[28] C. Zhang and Z. Fang, A new distributed intrusion detection system model based on SVM in wireless mesh networks, *Journal of Informatics and Computational Science* **12** (2015), 751–759.

[29] S.K. Biswas and M.M.M. Mia, Image reconstruction using multi layer perceptron and support vector machine classifier and study of classification accuracy, *International Journal on Science Technology and Research* **04** (2015), 226–231.

[30] J.A.K. Suykens, T. Van Gestel, De Brabanter, B. De Moor and J. Vandewalle, Least Squares Support Vector Machines, World Scientific, Singapore; (2002).

[31] R. Collobert and S. Bengio, Link between preceptrons, MLP and SVMs, In: *2004 International Conference on Machine Learning* (2004), 23–31.

[32] F. Kuang, W. Xu and S. Zhang, A novel hybrid KPCA and SVM with GA model for intrusion detection, *Applied Soft Computing* **18** (2014), 178–184.

[33] V.S. Feng and S.Y. Chang, Determination of a wireless networks parameters through parallel hierarchical support vector machines, *IEEE Transactions on Parallel and Distributed Systems* **23** (2012), 505–512.

[34] K. Jiang, J. Lu and K. Xia, A novel algorithm for imbalance data classification based on genetic algorithm improved smote, *Arabian Journal for Science and Engineering* **41** (2016), 3255–3266.

[35] P. Ganeshkumar and D. Devaraj, Intrusion detection using artificial neural network with reduced input features, *ICTACT Journal on Soft Computing* **1** (2010), 30–36.

[36] G. Creech and J. Hu, Generation of a new IDS test dataset: Time to retire the KDD collection. In: *Wireless Communication and Network 2013 International conference on IEEE* (2013), 4487–4492.

[37] L. Portnoy, E. Eskin and S. Stolfo, Intrusion detection with unlabelled data using clustering. In: *Proceeding of ACM CSS Workshop on Data Mining Applied to Security* (2001), 5–8.

[38] B. Mukherjee, L.T. Heberlein and K.N. Levitt, Network intrusion detection, *IEEE Network* **8.3** (1994), 26–41.