A Review of Soft Computing Solutions to Intrusion in Computer Network

Gargee Shukla
Dept. of Mathematics.
Govt J.P Vema P.G. Arts and commerce College
Bilaspur,C.G.

Anamika Shukla Sharma
Dept. of Computer Science,Govt. E.R.R P.G Science College,
Bilaspur, C.G.

Hari Shankar Hota
Dept. of Computer Science
Bilaspur University
Bilaspur, C.G

ABSTRACT
With the wide adoption of internet, there lies threat to sensitive information being shared on the network. An intrusion can be defined as an act or a number of acts in a sequence that either cause a compromise or intend to compromise the information. These intrusions need somehow to be detected so that the harm caused by them may be prevented. A system that keeps looking for activities in a computer or a network to detect intrusions is called an Intrusion Detection System (IDS).

Many novel methods of intrusion detection involve the use of Soft Computing tools. Soft Computing (SC) is a collection of methods used for developing intelligent systems for the problems for which conventional techniques have not given low cost or complete solutions. Artificial Neural Networks (ANN), Fuzzy Logic theory (FL) and Genetic Algorithm (GA) represent the most common tools of soft computing. The capability of soft computing tools to tolerate imprecision, partial truth, uncertainty and ability to provide low solution costs to real world problems and computationally intelligent problems are the obvious reasons which has made this approach widely accepted in field of Intrusion Detection

In this research work, we have collected about thirty papers to study how different soft computing tools and techniques can be utilized to develop efficient and robust Intrusion detection Systems.

Keywords
Soft Computing, Fuzzy Logic, Genetic Algorithm, Intrusion Detection System (IDS)

1. INTRODUCTION
An intrusion can be defined as an act or a number of acts in a sequence that either cause a compromise or intend to compromise the information. These intrusions need somehow to be detected so that the harm caused by them may be prevented. A system that keeps looking for activities in a computer or a network to detect intrusions is called an Intrusion Detection System. Many different approaches are used to prevent Intrusions in computer systems and networks; soft computing is one of them.

Soft computing is the name given to a combination of methodologies that helps finding solution of real world problems which are not easily modeled or cannot be modeled. It makes this possible by exploiting the tolerance for imprecision, uncertainty, approximate reasoning, and partial truth [1].

Other methods to detect intrusions include the concepts of Artificial intelligence (AI). One such example is Denning's profile model which is an expert system based intrusion detection model that performs rule-based analysis [2]. Dependence of rule-based analysis on a set of predefined rules supplied by the administrator or created by the systems has been reported by various authors [3]. This dependency gives rise to the need of updating these systems frequently to maintain their currentness [3][4].Another difficulty in such systems is encountered when rules directly dependent on audit data are derived[5] . As reported by many authors very minor changes in data may lead to condition of false positive and false negatives [5]. This means the IDS designed using such approach is usually inflexible and may be considered unreliable. To function correctly at a particular time, an expert system needs to be updated manually as it does not have learning capability like neural networks [3].Also, when intrusions span over a period of time they might not be detected by a rule based system. In order to understand how soft computing can be applied to the process of intrusion detection it is necessary to understand the basic model of an intrusion detection system (Fig.1).

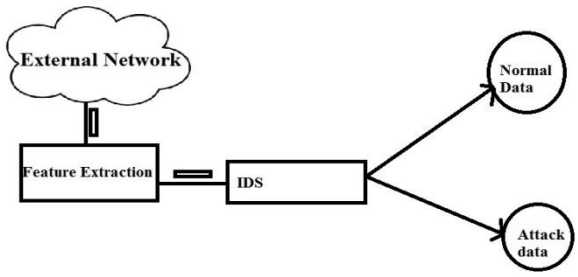

Fig. 1. Basic Model of IDS

Data is taken from external network and then based on the technique used by the IDS it is classified into normal or attack data and then according to this classification, actions are taken by the administrators. Intrusion detection systems can be classified in a variety of ways, the most common classification classifies each IDS into a Host-Based or a Network-Based IDS. Generally, a network-based IDS is configured by using a network node (or sensor) with a Network Interface Card (NIC) and an interface for management kept apart. This IDS is usually located in a segment or along the network border to check for intrusions by monitoring the traffic. Unlike the Network-based IDS Host-based IDS works by the use of small programs installed on each node to be monitored which have capabilities of monitoring the operating system, insert data in log files and raising alarms when required. Thus, Host-based IDS lacks the facility to monitor the network as a whole [6].Another Classification is based on the fact that most of the IDS act as pattern classifiers, they classify each pattern of data as either a normal pattern or a pattern signifying intrusions. Misuse

Detection, aims to detect the presence of a pattern matching to the prior representation of specific patterns for intrusions, allowing any matches to them in current activity to then be reported. Anomaly based Detection identifies the anomalies by matching the current patterns with the prior representation of normal behavior of users.

2. SOFT COMPUTING TECHNIQUES

Soft Computing tools and approaches are relatively newer techniques to be applied in the field of detecting Intrusions. Fuzzy logic, Genetic algorithms and Artificial Neural Networks are the commonly used tools of soft computing and are nowadays being used in various different fields to provide solutions to problems more efficiently at lower costs .

Fuzzy Logic is a tool for applying reasoning and uncertainty tolerance. It is a kind of "multi-valued logic". This capability of Fuzzy Logics can be utilized to write if-then rules for Intrusion Detection Systems.

Artificial Neural Networks are models or algorithms that mimic biological systems and used for learning a particular problem. This is mostly used in classification and as such neural networks can be used to classify activities under categories of normal or intrusive behavior for a system.

Support Vector Machines are also considered as a technique of soft computing by some authors.SVM (Support Vector Machines) are supervised learning models which are mostly used in the area of Intrusion Detection Systems for the purpose of classification.SVM is basically a classification algorithm that produces a hyper-plane as an output to classify data items which are represented by points in an m-dimensional feature space where, m is the number of features used for classifying the data items.

Genetic Algorithms are kind of algorithms inspired by biological systems and are used for optimization. Various authors have used it for optimization of features.

Hybrid Technique One can also combine two or more of these tools together to form a hybrid model for intrusion detection. This hybrid system will have capability of better learning, optimization and reasoning in a single Intrusion Detection System. This is the reason why the soft computing tools are generally combined to get an intrusion detection system. This paper focuses on various soft computing based technologies used to design intrusion detection systems.

3. LITERATURE REVIEW RELATED TO SUBJECT OF THE PAPER

Many authors have contributed their work towards the development of IDS using soft computing techniques. As stated we have collected thirty papers related to the subject of this paper from various well known journals, databases, which are explained in brief in the following part.

Feng et al (2014), proposed data classification algorithm which can be used for network IDS [7].The algorithm combines the best of SVM and Self-Organized Ant Colony Network (CSOACN) and tries to exclude the limitations of these approaches. The method used, uses binary SVM and the multiclass problem is solved by a clustering method that improves the average detection rate of all data classes. The authors have reported various advantages of using this method. As it used only the data points around the boundaries (support vectors) of two classes to construct the classifier in comparison with pure CSOACN, they found, the algorithm proposed takes less overall training time. When new sets of data arrive to the system, no classifier retraining is needed in the CSVAC (Combining Support Vector with Ant Colony) approach. According to the experiment results conducted for this model, the CSVAC algorithm outplays pure SVM in the experiments with higher average detection rate, less training time, and lower rates of both false negative and false positive; and it is better than pure CSOACN in terms of less training time with comparable detection rate and false alarm rates.

Another example of utilization of SVM in IDS for anomaly detection can be seen in the work of Song et al. (2009) [8].In which, the authors have proposed an anomaly detection method based on clustering and multiple one-class SVM in order to improve the detection rate while maintaining a low false positive rate. The evaluation results discussed in the work show that this approach outplays some existing algorithms reported in the literature; especially in detection of unknown attacks.

Another tool of soft computing, Neural Networks have been used by various authors for classification of normal and intrusive data .Intruders are challenging IDS creators day by day by a variety of attacks. It is rarely possible that all types of attacks in a network are known in advance. When an IDS faces such an environment it is better to take advantage of unsupervised classification offered by another tool of soft computing, Neural networks. .A good example has been laid by Hoz et al(2015) by the use of Probabilistic Self-Organizing Maps (PSOM) to model the feature space and enable distinguishing between normal and anomalous connections[9]. The main advantage of the approach proposed is, the detection capabilities of system proposed can be modified without retraining the map, but only by modifying the unit's activation probabilities this property helps avoiding the execution of the entire training process for news samples.

Ibrahim et al. (2013) have utilized Artificial Neural Network for unsupervised classification .It is a hierarchical Anomaly Intrusion Detection System and uses SOM neural nets for detection and separation of normal traffic from the attack traffic [10]. Experiments conducted and given in the text of this work show that SOM with KDD99 is 92.37% able to recognize attack traffic from normal one, while with NSL-KDD is 75.49% able to recognize attack traffic from normal one thus when KDD99 network intrusion dataset is taken SOM are best suited due to their high speed and fast conversion rates as compared with other learning techniques. Authors have also found that using SOM obtains superior performance in comparison with other state-of-the-art detection methods.

The situations calling for supervised classification of network data have also benefitted from neural networks. A work by Sondhiya et al. (2013) shows the use of Multi Layer Perceptron to detect intrusions in Cloud computing for protecting each Virtual machine against intrusions, to achieve both effectiveness of using the system resource and strength of the security service without trade-off between them [11].

A work by S. Devaraju, S. Ramakrishnan (2013) can be seen as a support in the use of neural networks as classifiers in IDSs [12]. The work comprises a comparison of the performances of intrusion detection with Feed Forward Neural Network (FFNN), Elman Neural Network (ENN), Generalized Regression Neural Network (GRNN), Probabilistic Neural Network (PNN) and Radial Basis Neural Network (RBNN).PCA was used for feature reduction in KDDCUP99 dataset and 41 features were reduced into 13 features. The Probabilistic Neural Network provided the best

accuracy among the other classifiers used. A similar study was done by the authors in the year 2014 too, which proved that the FFNN, GRNN and PNN provide better accuracy over other approaches for DoS attack, PNN provides better accuracy over other approaches for Probe attack, and FFNN provides better accuracy over other approaches for R2L attacks and U2R attacks[13]. The authors have proposed to consider FFNN techniques to improve the efficiency and reduce the false alarm rate.

It can be easily implied various kind of approaches, neural networks and other classifiers have their own advantages in their use. This seems the obvious reason why various authors have proposed ensemble based approaches .One such work was done by Gowrin et al. (2013) [14] . Considering the importance of computational complexity of Intrusion Detection algorithms the authors designed an intrusion detection system to classify data by the incorporation of enhanced rules as learnt from the network behavior with less computational complexity of O (n). The back propagation neural network model is considered for the experimental model proposed which consisted of 41 inputs, 1 bias, 31 hidden neurons and 22 output neuron. A lot of classifiers were compared by them and it was found that, the neural network based (being a weak classifier) Adaboost algorithm (strong classifier) performed well in the experimentation with KDD Cup99 data. If T iterations are required to construct the strong classifier, the computational complexity of testing a data is O (T) as reported by them.

Another work by Veerwal et al. (2013) shows an Ensemble of Soft Computing Techniques for Intrusion Detection[15]. In an experiment they have fused two different Multi Layer Feed Forward Neural Networks trained using two different training algorithms and one Support Vector Machine. They analyzed three fusion strategies, namely Dempster Shafer Theory based Fusion, Bayesian Fusion and Neural Network Combination. Dataset was trained and tested on individual classifier as well as on the multiple fused classifiers. In the work being referred, they had experimented ensemble IDSs with three different fusion techniques. As per the authors, Multiple Classifier Fusion approach provided better accuracy with low false alarm generation than that provided by an individual classifier trained on the training data set. The authors also inferred Multi classifier paradigms do not always give better performance, in some cases when the evidence is highly conflicting some fusion strategies fail. Out of the three fusion techniques, Dempster Shafer Theory based fusion performed the best in the experiment. So instead of developing an accurate classifier the authors suggested many weak classifiers and combining them using Dempster Shafer Theory to get a good result in terms of accuracy and low false alarm rate.

Another property of soft computing that is widely being utilized in the field of intrusion detection is its tolerance for uncertainty and imprecision. This property is offered by Fuzzy Logic. This tool was utilized in the work of Amini et al. (2014) who proposed an ensemble method with neural networks for intrusion detection based on fuzzy clustering and stacking combination method [16]. The authors used fuzzy clustering for dividing the dataset into more homogeneous portions which reduces the complexity of training and causes the models to have more accurate classifications and a stacking combination method to aggregate the predictions of base models and reduce their errors to enhance the accuracy for detection. Radial basis Function (RBF) is used in this work as base classifier which helped avoiding the problem of getting stuck into a local maximum and Multi-Layer Perceptron (MLP) neural networks to aggregate the predictions of all ensemble members thus making the prediction obtained to be stable. RBF networks are trained in this model based on different subsets of the whole network traffic. The results of experiments carried on NSL-KDD dataset demonstrated the fact that, the performance of the proposed ensemble method is higher compared to other well-known classification techniques, particularly when the classes of attacks are small (U2R, R2L and PRB which are difficult for classification). They also have shown this way, the use of a hybrid combination method and a stacking procedure increases the detection performance of the ensemble model.

El-Sayed et al.(2014) utilized multicriterion decision making fuzzy classification, known as PROAFTN [17][18] combined with a greedy hill-climbing search for attribute selection for designing a new methodology for anomaly-based intrusion detection[19]. According to them the anomaly-based intrusion detection problem can be solved by a multicriterion fuzzy classification approach which assigns behavioral patterns to predefined classes. The evaluation in the work is performed by comparing the alternatives to different prototypes of classes, where the category or class is assigned to patterns based on the highest score value. The results of the experiments conducted in this work have shown that more than 99.9% overall accuracy with high detection rates for various types of intrusions can be achieved with about 26% only of the available attributes.

The application of fuzzy concepts is not restricted to a particular network. This is evident from the work of Vishnu Balan et al., (2015) who have suggested Fuzzy Based Intrusion Detection Systems for mobile ad-hoc networks [20]. The authors proposed a system that detects the malicious behavior of node by intrusion detection system and also identifies the type of attack. The system basically detects attacks such as black hole attack and gray hole attack and is also able to prevent those kind of attacks by using node blocking mechanism such that the proposed system provides a secure communication between nodes.

Another example where fuzzy logic is used in developing intrusion detection system is the Fuzzy Intrusion Recognition Engine (FIRE) [21]. It is an anomaly-based intrusion detection system that uses fuzzy logic to assess whether malicious activity is taking place on a network. Data mining techniques are used to process the network input data and help expose metrics that are particularly significant to anomaly detection which are then, evaluated as fuzzy sets. A fuzzy analysis engine is present to evaluate the fuzzy inputs and trigger alert levels for the security administrator. Fire was initially tested on production local area networks in the College of Engineering at Iowa State University. It was found by the authors that, it can detect a wide range of common attack types. The fuzzy rule described by the authors in the work allowed FIRE to detect nine distinct TCP port scans and four separate ICMP (ping) scans of hosts on the network by potentially malicious attackers from outside the local network domain. It was also found able to detect non malicious port scans launched against the system from the local domain. Using the fuzzy rules described by the authors they also found, it was successful in triggering HIGH alerts when rarely seen types of network traffic were observed.

Shamshirband et al (2014) used fuzzy logic in a hybrid intrusion detection system called Fuzzy Q-learning (FQL) algorithm proposed by them to protect wireless nodes within the network and target nodes from DdoS attacks to identify

the attack patterns, take appropriate countermeasures [22]. The work, fuzzy logic controller utilized fuzzy min-max strategy to provide the action selection policy. The Q-learning algorithm was used by the authors for adjusting the parameters (i.e, state, action) based on fuzzy functions to reduce the complexity of states and action as well as speed up the decision process. The proposed system was trained and tested to check its performance by generating attacks from the NSL-KDD and CAIDA DdoS attack datasets during the simulation experiments. Results of these experiments had shown that the proposed IDS has higher accuracy of detection rate than Fuzzy Logic Controller and Q-learning algorithm This work successfully described how DdoS attacks launched in wireless network can be modeled through fuzzy Q-learning algorithms.

Evaluation of three fuzzy rule based classifiers(FR1,FR2,FR3) was done in the work of Ajith Abraham et al (2004) who also modeled Soft Computing(SC) based IDS (SCIDS) as a combination of different classifiers to model lightweight (using 12 attributes) and more accurate heavy weight (using 41 attributes) IDS [23]. According to some findings authors suggested the use of light weight SCIDS for MANET/distributed systems and the heavy weight SCIDS for conventional static networks, wireless base stations etc. One of the fuzzy classifier (FR2) gave 100% accuracy for all attack types using all the 41 attributes.

Intrusion detection systems involve a number of parameters and also require them to be optimized. Genetic algorithm has been used by the researches in the field of intrusion detection for optimization of parameters and variety of reasons as given in the following paragraphs.

Ahmad et al., (2014) considered selection of an appropriate number of principal components is a critical problem in subset selection which was the reason they applied GA to search the genetic principal components that offered a subset of features with optimal sensitivity and the highest discriminatory power [24]. The model proposed in their work, uses SVM for the purpose of classification. The method proposed was found to be providing optimal performance in intrusion detection which is capable to minimize amount of features and maximize the detection rates.

Another work that utilizes classification by SVM and Genetic algorithms optimization capability is a work by Kuang et al.(2014) who proposed support vector machine (SVM) model combining kernel principal component analysis (KPCA) with genetic algorithm (GA) for intrusion detection[25]. In the model proposed by them, a multi-layer SVM classifier is adopted to estimate whether the action is an attack; GA is employed to optimize the punishment factor C, kernel parameters and the tube size ε of SVM. The results of the experiment conducted in the work have shown, the classification accuracies of the proposed KPCA SVM model are superior to those of SVM classifiers whose parameters are randomly selected.

According to the some authors, user profile does not remain the same at all the time, so they have used Genetic Algorithm to observe the different variations possible in a user's profile using it to generate a new data by applying mutation operation on the existing dataset to produce a new dataset [26].

Some other authors have applied the combination of soft computing tools to intrusion detection models and were successful in designing efficient intrusion detection systems. Bridges and Vaughn (2000) described a prototype intelligent intrusion detection system (IIDS) that was being developed that time to demonstrate the effectiveness of data mining techniques that utilize fuzzy logic and genetic algorithms [27]. The system proposed, combined both anomaly based intrusion detection using fuzzy data mining techniques and misuse detection using traditional rule-based expert system techniques. Genetic Algorithm was utilized to, tune the fuzzy membership functions to improve performance, and select the set of features available from the audit data that provide the most information to the data mining component. Various authors have reported that, if one derives rules that are directly dependent on audit data, an intrusion that deviates only slightly from a pattern derived from the audit data may not be detected or a small change in normal behavior may cause a false alarm. This problem was addressed in the proposed system by integrating fuzzy logic with data mining methods for intrusion detection.

The use of genetic algorithm to tune the membership functions of the fuzzy variables used to mine the fuzzy association rules is described in the work of Wang & Bridges (2000), in order to improve the performance of the intrusion detection system. The system proposed has been trained and tested using three sets of network traffic data downloaded from http://iris.cs.uml.edu:8080.These three data sets were collected by tcpdump. The experiments conducted in this work, have shown improved performance in detecting network intrusion [28].

Another work that uses Genetic fuzzy systems is the work by Elhag et al, (2015) which describes the use of Genetic Fuzzy Systems within a pair wise learning framework. According to the authors, the use of fuzzy sets, and especially linguistic labels, enables a smoother borderline between the concepts, and allows a higher interpretability of the rule set which provides an advantage to the system .Results of the experiments carried on KDDCUP'99 have shown that proposed approach has the best tradeoff among all performance measures. The authors have also stated, the use of fuzzy logic as a tool allows addressing the vague division that exists between normal and anomalous accesses properly [29].

Kumar and Selvakumar, (2013) suggested an algorithm for classifying DDOS attacks. The DDoS classification algorithm, NFBoost, as they proposed, differs from the existing methods in weight update distribution strategy, error cost minimization, and ensemble output combination method, but resembles similar in classifier weight assignment and error computation [30]. The drawbacks of interpretability and manual rules acquisition were eradicated by using Hybrid methods, Neuro-fuzzy and genetic fuzzy. In the text provided by the authors adaptive and hybrid neuro-fuzzy systems were proposed as subsystems of the ensemble. Detection accuracy and Cost per sample were the two metrics used to analyze the performance of the NFBoost classification algorithm and it was compared with bagging, boosting, and AdaBoost algorithms. From the simulation results, it was inferred that NFBoost algorithm achieved high detection accuracy (99.2%) with fewer false alarms. Cost per instance was also very less for the NFBoost algorithm compared to the existing algorithms.

4. CONCLUSION

In this paper we have presented review of soft computing techniques, approaches and methodologies in Intrusion Detection Systems used in recent years, focusing on how they are applied in Intrusion Detection Systems. The capability of

soft computing tools to tolerate imprecision, partial truth, uncertainty and ability to provide low solution costs to real world problems and computationally intelligent problems are the obvious reasons which has made this approach widely accepted in field of Intrusion Detection. The paper presented how soft computing is applied to every type of network and any type of network technology. Soft computing methods are used to aid performances of the other classifiers. Not only various soft computing tools can be combined to form a hybrid system which can be used to provide a solution but, ensemble of different classifiers soft computing methodology, can also provide promising solutions.

5. REFERENCES

[1] Zadeh Lofty A. 1994, Soft computing and fuzzy logic, IEEE Software, Volume 11 Issue 6, 46-58.

[2] Denning, D.E. 1987, IEEE Transactions on Software Engineering , Vol. Se-13, No. 2, February 1987, pp 222-232.

[3] Cannady, J. 1998, Applying Neural Networks to Misuse Detection. In Proceedings of the 21st National Information Systems Security Conference.

[4] Sebring, M., Shellhouse, E., Hanna, M. & Whitehurst, R. 1988, Expert Systems in Intrusion Detection: A Case Study, Proceedings of the 11th National Computer Security Conference 1988.

[5] Guan J., Liu D.-X, Wang T 2004, Applications of fuzzy data mining methods for intrusion detection systems, Computational Science and Its Applications - ICCSA 2004: International conference assisi Italy may 2004 proceedings part III.

[6] Examining Different Types of Intrusion Detection Systems 2014. Retrieved from http://www.dummies.com/how-to/content/examining-different-types-of-intrusion-detection-s.html

[7] Feng W, Zhang Q, Hu G., Huang J.X. 2014, Mining network data for intrusion detection through combining SVMs with ant colony networks, Future Generation Computer Systems ,37 ,2014, 127–140.

[8] Song J., Takakura H., Okabe Y., Kwon Y.2009, Unsupervised Anomaly Detection Based on Clustering and Multiple One-class SVM, IEICE Transactions on Communications E92-B (06) ,2009, 1981–1990.

[9] Hoz, D. l., Hoz, D. L., Ortiz, A., Ortega, J., & Prieto, B. (n.d.) 2015, PCA filtering and probabilistic SOM for network intrusion detection , Neurocomputing, , 164(21), September 2015, pp 71–81

[10] Ibrahim, L. M., Basheer, D. T., & Mahmod, S. (n.d.) 2013. A Comparison Study For Intrusion Database (Kdd99, Nsl-Kdd) Based On Self Organization Map (Som) Artificial Neural Network Journal of Engineering Science and Technology,8(1),107 - 119

[11] Sondhiya R., Shreevastav M., Mishra M. 2013,To Improve Security in Cloud Computing with Intrusion detection system using Neural Network International Journal of Soft Computing and Engineering (IJSCE), 3(2), May 2013.

[12] Devaraju S., Ramakrishnan S. 2013 , Detection of Accuracy For Intrusion Detection System Using Neural Network Classifier, International Journal of Emerging Technology and Advanced Engineering, 3(1), January 2013.

[13] Devaraju S., Ramakrishnan S. 2014,Performance Comparison For Intrusion Detection System Using Neural Network With Kdd Dataset ,ICTACT Journal On Soft Computing, April 2014, 04(03).

[14] Gowrison G., Ramar K, Muneeswaran K., Revathi T.2013, Minimal complexity attack classification intrusion detection system, Applied Soft Computing, 13, 2013, 921–927.

[15] Veerwal D., Choudhary N. & Singh D., Ensemble of Soft Computing Techniques for Intrusion Detection 2013. Global Journal of Computer Science and Technology Network, Web & Security, 13(13),2013

[16] Amini, M., Rezaeenoor, J., & Hadav, E. (n.d.).2014, Effective Intrusion Detection with a Neural Network Ensemble Using Fuzzy Clustering and Stacking Combination Method ,Journal of Computing and Security, Volume 1, Number 4 ,293-305 ,October 2014.

[17] Belacel N. 2000,Multicriteria assignment method PROAFTN: Methodology and medical application, European Journal of Operational Research 2000; 125 (1) ,175 – 183.

[18] Al-Obeidat F., Belacel, N., Carretero, J.A., Mahanti, P. 2011, An evolutionary framework using particle swarm optimization for classification method PROAFTN., Applied Soft Computing 2011;11(8):4971 – 4980.

[19] El-Alfy, E.-S. M., & Al-Obeidat, F. N. (n.d.) 2014. A multicriterion fuzzy classification method with greedy attribute selection for anomaly-based intrusion detection ,Procedia Computer Science 34 ,2014, 55 – 62.

[20] Balan, E. V., Priyan, M. K., C., G., & Devi, G. U. (n.d.).2015, Fuzzy Based Intrusion Detection Systems in MANET , Procedia Computer Science,2nd International Symposium on Big Data and Cloud Computing. ,50 ,2015, 109 – 114

[21] Dickerson, J. E. and Dickerson J. A. 2000 ,Fuzzy network profiling for intrusion detection. In Proc. of NAFIPS 19th International Confer-ence of the North American Fuzzy Information Processing Society At-lanta ,301–306.

[22] Shamshirband, S., Anuar, N. B., Kiah, L. M., & Misra, S. (n.d.). 2014, Anomaly Detection using Fuzzy Q-learning Algorithm , Acta Polytechnica Hungarica Vol. 11(8), 2014.

[23] Abraham, A., Jain, R., Sanyal, S., & Han, S. Y. (n.d.)., SCIDS: A Soft Computing Intrusion Detection System, Chapter Distributed Computing - IWDC 2004,Volume 3326 of the series Lecture Notes in Computer Science, 252-257

[24] Ahmad I., Hussain M. ,Alghamdi A., Alelaiwi A. 2014, Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components, Neural Computing & Applications, 24(7), 1671-1682.

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

[26] Murthy, Y. V., Harish, K., Varma, D. K., Sriram, K., & Revanth, B. V. (n.d.) 2014.Hybrid Intelligent Intrusion Detection System using Bayesian and Genetic Algorithm (BAGA): Comparitive Study International Journal of Computer Applications ,99 (2), August 2014 .

[27] Bridges Susan M., Vaughn Rayford B.2000, Fuzzy Data Mining And Genetic Algorithms Applied To Intrusion Detection Presented at the National Information Systems Security Conference (NISSC), October 16-19, 2000, Baltimore, MD.

[28] Wang Wengdong , Susan M. Bridges 2000,Genetic Algorithm Optimization of Membership Functions for Mining Fuzzy Association Rules , Presented at the International Joint Conference on Information Systems, Fuzzy Theory and Technology Conference, Atlantic City, N.J. March 2, 2000.

[29] Elhag S. , Fernandez A., Bawakid A. , Alshomrani S. , Herrera F. 2015, On the combination of genetic fuzzy systems and pair wise learning for improving detection rates on Intrusion Detection Systems Expert Systems with Applications, 42 ,193–202,2015.

[30] P. Arun Raj Kumar, Selvakumar 2013, Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems, Computer Communications , 36(3),2013, 303–319.