Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/081L09

Performance Analysis on Competitive, Roulette Wheel and Pseudo-Random Rules for Intrusion Detection

Ruey-Maw Chen *

Department of Computer Science and Information Engineering, NCUT, Taichung 41170, Taiwan, ROC

Received: 15 Apr. 2013, Revised: 10 Aug. 2013, Accepted: 11 Aug. 2013
Published online: 1 Apr. 2014

Abstract: Intrusion detection is a critical component of network security; detection schemes fundamentally use the observed characteristics of network packets as a basis for such determinations. Meanwhile, intrusion detection can be regarded as a clustering problem; many clustering schemes have been applied for classifying network packets. Among them, back propagation networks (BPN) and fuzzy c-means (FCM) are popular and well applied. Both of these schemes are based on a competitive characteristic. Nevertheless, a competitive characteristic may cause inappropriate clustering results for intrusion detection. Hence, in this study, different clustering criteria are proposed and adopted in BPN and FCM for classifying intrusion packet type; they are the roulette wheel selection rule and pseudo-random rule. Moreover, KDDCUP99 data sets were used as the evaluation packet samples of the experiments, and the given 41 packet features are reduced to 9, 11 and 24 key features for experimentation. Simulation results demonstrate that the proposed intrusion detection criteria applied in BPN yields higher detection rates for the U2R and R2L connections; misclassification of U2R and R2L connections would allow greater damage. Additionally, the suggested roulette wheel selection rule and pseudo-random rule intrusion detection criteria integrated into BPN are superior to other schemes with only 11 features used further reducing complexity and computation time.

Keywords: Intrusion detection, back propagation networks, fuzzy c-means, competitive, roulette wheel, pseudo-random rule

1 Introduction

Along with the development of the Internet's residing data, any data information or resources can make use of the network to facilitate quick and inexpensive delivery. However, massive use of the Internet has brought about various problems at the same time, such as spam, network worms, malicious code, malware and so forth. Among derived network problems, network security is one such important problem; how to tighten internet security has given rise to much attention by researchers. In the field of network security, detection of measures directed against a variety of network packet intrusion modes has become a very important subject. The main purpose of intrusion detection is to detect network security incidents in advance, thus preventing and countering the result of abnormal behaviour on the computer system or network [1]. Sadly, it is difficult to completely detect and prevent Internet attacks against possible intrusion. Therefore, how to increase the intrusion detection rate under increasingly sophisticated methods of attack has become a critical network security issue. Most intrusion detection technologies lean toward improving the detection rate and lowering the false positive rate, and thus the detection sensitivity will increase. Nevertheless, it will cause problems with excessive alarm messages, and still generate a large number of false positives. On the other hand, lowering the detection sensitivity in order to reduce false positives may allow some attacks to go undetected and result in false negatives. Therefore, how to achieve high detection rate and low false alarm rate (for both false positives and false negatives) is the goal of intrusion detection development. Intrusion detection technologies can be broadly divided into two types: anomaly detection and misuse detection. Anomaly detection utilizes a variety of abnormal packet statistics and summarizes the behaviour of normal system users or the normal network packet mode to establish appropriate patterns of behaviour in the system database. The behaviour judgement of the detection is compared against the database with the existing mode; large variation is considered abnormal. Advantages of this method are the high detection rate and the ability to detect new attacks;

* Corresponding author e-mail: raymond@ncut.edu.tw

however, the disadvantages are having more false positives and greater computing power required for summarizing. Related to anomaly detection, misuse detection is the use of a rule-based system in the definition of abnormal behaviour or abnormal network packet signature. The advantage is ability to accurately measure the known attack packets. However, the disadvantage is inability to identify new types of attack packets, and despite having a lower false positive rate, the false negative rate is high [2]. This work focuses on anomaly detection to yield high detection rates. Neural networks and fuzzy c-means (FCM) based schemes are used as tools for intrusion detection analysis to determine whether packets are normal or abnormal. In recent years, numerous researchers have presented many different methods for intrusion analysis. Khan *et al.* [3] proposed use of support vector machines (SVM) as an intrusion detection method. In a rule-based scheme as in [4], the event is described in a variety of syntax to create the event rule based analysis system. The system receiving a packet in compliance with attack rules indicates the occurrence of attacks. An anomalous detection technique combined with conditional legitimate probability was proposed for distributed intrusion prevention [5]. Meanwhile, data mining based technology was suggested for misuse and abnormal detections [6]. Recently, the back propagation network (BPN) scheme has been a well-known clustering technology; it has been successfully applied for classifying packets as normal or abnormal with high efficiency [7]. Furthermore, fuzzy c-means (FCM) is famed for its clustering characteristics which has also been improved upon and applied by Jiang *et al.* [8] for intrusion detection. The final intrusion determination of these two important clustering schemes is on the basis of a competitive rule; however, a competitive characteristic may cause impropriate clustering. However, the clustering criteria based on roulette wheel selection and a pseudo random rule inspired from ant colony optimization algorithm and roulette wheel selection have not been integrated in FCM. Meanwhile, most BPN clustering applications are based on the competitive characteristic; the roulette wheel scheme and pseudo random rule are not exploited to be the clustering criteria in BPN. Hence, in this study, a BPN and FCM schemes are applied for classifying packets as normal or abnormal. Additionally, extra decision mechanisms such as roulette wheel selection and pseudo-random rules are integrated into BPN and FCM for intrusion detection analysis. The selection of packet features and analysis schemes are the important factors that influence intrusion detection. Hence, different packet features (9, 11, and 24 features) are tested for performance evaluation. The detection performances of different decision criteria are also provided.

2 Detection Scheme and Framework

This study explores four types of network packet detection based on BPN and FCM techniques and analyses their detection performance on distinct detection decision criteria.

2.1 Fuzzy C-means

The Fuzzy c-means (FCM) clustering algorithm is successful and widely used in a variety of applications. These applications include image segmentation, speech recognition, and data compression. A fuzzy clustering one in which clusters are fuzzy subsets rather than crisp subsets of the collection was introduced by Zadeh [9]. Based on Bezdek [10], the fuzzy c-means clustering method is specified as follows: the fuzzy clustering method assigns each sample a number between zero and one indicating the degree of uncertainty described by *membership grade*. Samples that are similar to each other in the same cluster are identified by high membership grade. The membership grade displayed by μ_{xi} indicates the degree of possibility that x belongs to the ith fuzzy cluster. The x is a p-dimensional sample and is correlated to a packet with p features to be classified in this study. The membership grade is a value between zero and one which satisfies

$$\sum_{i=1}^{c} \mu_{xi} = 1, \; for\ x = 1,2,3...n\ and \tag{1}$$

$$0 < \sum_{x=1}^{n} \mu_{xi} < n, \; for\ i = 1,2,3,...c \tag{2}$$

Given a fuzzy partition P, the c centers, v_i i=$1,2,3,...,c$ associated with the partition are calculated by the following formula, as indicated in Eq.(3):

$$v_i = \frac{\sum_{x=1}^{n} [\mu_{xi}]^m z_x}{\sum_{x=1}^{n} [\mu_{xi}]^m} \quad for\ i = 1,2,3,...c \tag{3}$$

Where m is identified as the *fuzzification parameter* (or *exponential weight*) and is used to dominate the influence of membership grade and therefore the cluster centers. The c clusters correspond to the packet type in this study. As shown by Bezdek [10], the developed fuzzy c-means algorithm updates the membership grade by the following procedure:

$$\mu_{xi} = \sum_{j=1}^{c} \left[\frac{\|z_x - v_i\|^2}{\|z_x - v_j\|^2} \right]^{\frac{-1}{m-1}} \tag{4}$$

2.2 Roulette Wheel Method Decision in FCM

The conventional classification decision in FCM is directly determined by the maximum membership grade.

Restated, the packet type is the one with the maximum membership grade. However, there are some characteristics of certain data packets often causing false positives, *i.e.*, the membership grades have small gaps. Therefore, to reduce misclassification, the final decision of the classification in FCM is modified. Instead of using the FCMs conventional decision criterion, a decision scheme commonly used in genetic algorithms for selecting genes, known as the roulette wheel selection, is proposed. The process of the roulette wheel selection method combined with FCM is as follows: normalize the membership grade μ_{xi} $(i = 1 \sim c)$ when the termination condition is met, then the selection probability p_{xi} for cluster c is determined as in Eq. (5), followed by the roulette wheel selection method.

$$p_{xi} = \frac{\mu_{xi}}{\sum_{i=1}^{c} \mu_{xi}} \tag{5}$$

Restated, packet x is categorized into intrusion type k when $r < \sum_{i=1}^{k} p_{xi}$, where r is a random generated number, $r \in (0,1)$. In this work, a local search inspired from the greedy randomized adaptive search procedure is adopted for roulette wheel selection, and is named the greedy roulette wheel selection (GRW) method.

2.3 Pseudo-Random Rule Determination in FCM

The roulette wheel selection rule is sometimes too random. Alternatively, a compromise between competitive determination and the roulette wheel selection rule is proposed for classifying the pseudo-random rule. The pseudo-random rule is used in ant colony optimization (ACO), which was first suggested by Dorigo and Gambardella [11] in order to increase the exploitation ability for improved solution quality. In ACO, when a generated random number q is less than or equal to the predefined constant q_0, then select the path with the maximum pheromone and heuristics directing toward the best path; this is so-called exploitation. Conversely, if q is greater than q_0, then search for a path other than the best path found so far. This is known as exploration. Restated, this concept of balancing exploitation and exploration is applied into back propagation neural networks for deciding what intrusion type the packet should be classified as, such that data likely caused false positives but could probably have been classified correctly. The pseudo-random rule in ACO is displayed in Eq. (6).

$$j = \begin{cases} arg\ max \left\{ (\tau(x,i))^{\alpha} (\eta(x,i))^{\beta} \right\}, & q \leqslant q_0 \\ J, & q > q_0 \end{cases} \tag{6}$$

Where, $\tau(x,i)$ and $\eta(x,i)$ in Eq. (6) are the pheromone and heuristic, respectively; α, β denote the parameters correlating to the importance of the pheromone and heuristic. In this study, the pseudo-random proportional rule in the "exploitation" step is modified as: the node with maximum output value falls into that specific cluster when $q \leq q_0$. The rule of the "exploration" step is changed to using roulette wheel selection when $q > q_0$. Meanwhile, the membership grade is regarded as the pheromone in ACO; is set to 1. Hence, when $q > q_0$, the membership grade of μ_{xi} is associated with a probability pj which is determined using Eq. (5) starting from the 1st group, then accumulating the value of p_j. The packet type is then determined when the cumulated probability is greater than a random generated number r, $r \in (0,1)$, i.e., $r \leq \sum_{j=1}^{k} p_k$. The clustering process based on the pseudo-random rule is designed as follows.

$$j = \begin{cases} arg\ max\,[\mu_{xi}], & q \leqslant q_0 \\ J, & q > q_0 \end{cases} \tag{7}$$

Where,
- μ_{xi}: the membership grade of packet x in the ith packet type;
- J: determined by the roulette wheel;
- q: 0 to 1, the generated random number;
- q_0: predefined parameter.

2.4 Back Propagation Networks

Supervised neural networks are suitable for use in diagnosis, prediction and classification. In this work, the roulette selection method and pseudo-random rule, combined with supervised back propagation neural networks are proposed as the identification method in intrusion packet detection. The back propagation neural network is one of the most commonly used supervised neural network models and uses feedback information as its learning mechanism. The back propagation neural network is essentially a network of simple processing elements working together to produce complex output. These elements (or nodes) are arranged into different layers: input, hidden, and output layers. The input layer propagates a particular input vectors components to each node in the hidden layer. The number of nodes (neurons) corresponds to the number of network packet characteristics. Hidden layer nodes compute output values, which become input for the nodes of the output layer. The output layer nodes compute the network output for the particular input vector. The quantity of nodes corresponds to the number of packet types to be classified.

- X_i: the variables of each input layer $(i = 1,2,.,n)$; corresponding to packet features in this work;
- W_{ik}: the weights between the input layer and hidden layer $(k = 1,2,.,m)$;
- W_{kj}: the weights between the hidden layer and output layer $(j = 1,2,.,p)$;

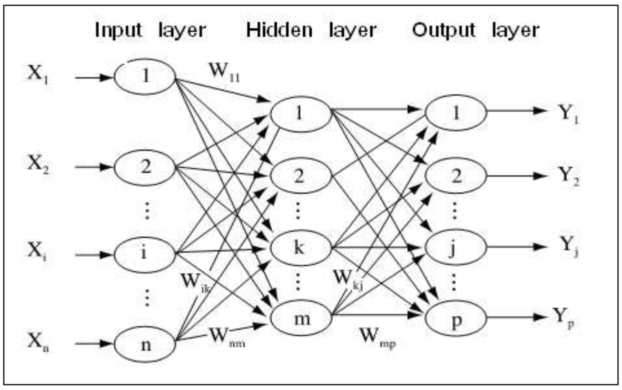

Fig. 1: Neural network learning architecture diagram [9]

• Y_j: the variables of the output layer; associated with the packet types to be classified in this work.

The BPN uses training samples to train the network to learn the weights between nodes, adjusting the synaptic strengths among nodes and between layers until the network output value is close to the target value. Most of the intrusion detection techniques require training data to ensure their detection performance. BPN relies on accurate and fast recall of learned characteristics; hence, application of BPN is applied in a variety of complex attack classifications. Basically, the classification output determination in conventional BPN is on the basis of competition, with the neuron having the biggest output neuron state value being the activated neuron.

2.5 Roulette Wheel Method Decision in BPN

The processes of the roulette wheel selection method are similar to that applied in FCM. Restated, the operation of roulette wheel selection in BPN is as follows: normalize the output of $Y_j (j = 1 \sim p)$ in the output layer, then the selection probability pj for cluster j is determined as in Eq. (8), followed by the roulette wheel selection method.

$$p_j = \frac{Y_j}{\sum_{i=1}^{p} Y_i} \tag{8}$$

Restated, the packet is categorized into intrusion type k when $r \leq \sum_{j=1}^{k} p_j$, where r is a random generated number and $r \in (0,1)$.

2.6 Pseudo-Random Rule Determination in BPN

Similarly, the pseudo-random proportional rule in the “exploitation” step is applied in BPN and is modified as: the node with maximum output value in that specific cluster when $q \leq q_0$. The rule of the “exploration” step is changed to using roulette wheel selection when $q > q_0$. Hence, when $q > q_0$, the value of Y_j is associated with a probability pj which is determined using Eq. (8). The clustering process in BPN is as follows.

$$j = \begin{cases} arg\,max\,[Y_j]\,, & q \leqslant q_0 \\ J, & q > q_0 \end{cases} \tag{9}$$

3 Experiment and Analysis

In this study, the training data sample packets and test samples of packet data from the data set of KDDCup’99 were selected. Then a feature selection method was used to filter out less important characteristics and noise, thus reducing the overall amount of data. Next, the pre-processing stage and data normalization were conducted, and finally normalized data was used for the intrusion detection experiment and analysis. The KDDCup’99 dataset is prepared and managed by MIT Lincoln Labs [12] with the objective to evaluate and survey research in intrusion detection. The KDDCup’99 data set contains 41 features that describe a connection and one target class feature for each packet. Features 1-9 stand for the basic features of a packet, 10-22 for content features, 23-31 for traffic features and 32-41 for host-based features. There are 7 nominal and 34 continuous features. In all, the dataset includes 4,898,431 packet records and can be divided into four categories of attack: Probe, DoS, U2R, and R2L. Including the normal network packets, these five packet types will be classified as a type of intrusion detection. Two of five classes are considered rare; U2R and R2L classes represent 0.4% and 5.7% of the entire population, respectively. Restated, learning from these two packet types is difficult and infeasible. Meanwhile, misclassification of these two packet types would be costly. In this work, kddcup.data_10_percent.gz packet data are picked for training and test sets. It contains 10% of the amount of data of KDDCup99 for a total of 494,021 communication records. The first phase of the experiment is collecting packet data. There are 15,000 (among 494,021) communication records selected as training data, and another 15,000 (among 494,021) communication records are selected as test data. Both training and test data are randomly selected from KDDCup’99. The selection of packet features and analysis schemes are the important factors that influence intrusion detection. Hence, the second phase is to select desired features of the packets. Each data packet in the KDDCup’99 data set contains 41 feature values. However, feature selection has to be filtered since not all the characteristics of the packet have decisive influence on clustering results. Too many features may cause false positives during data clustering. Therefore, the number of filtered characteristics is an important factor in detection performance. In this study, the 41 features of KDDCup’99 will be reduced to 9, 11 and 24 features. Restated, this work reduced data dimensionality and complexity and filtered out less important features before testing. The third phase is the data preprocessing, with the selected features including numeric and categorical types of features. Hence, the characteristics of the categories were replaced by the corresponding values. Meanwhile, the numeric data are converted into values between 0 and 1 in order to avoid producing false results due to large differences of data.

In fuzzy c-means, the packets have 9, 11 and 24 features; the number of clusters is 5, *i.e.*, c=5, corresponding to Normal, Probe, DoS, U2R, and R2L category packets. Additionally, the predefined parameter q_0 used in the pseudo-random rule is set to 0.9 which is obtained after several tests. The performance evaluation for the algorithms is based on the detection rate as defined in Eq. (10). The simulation results are listed in Tables I and II.

$$Decision\ rate = \frac{Detected\ attacks}{Number\ of\ attacks} * 100\% \qquad (10)$$

Tables I, II and III display the performance using different classification methods applied in FCM and different numbers of features. Meanwhile, Tables IV-VI display the detection rates of using the proposed schemes in BPN. Additionally, the average detection rates of the studied methods are illustrates in Figures 2 and 3.

Table I. FCM experimental results of 9 features (%)

Packet type	*Normal*	*Probe*	*DoS*	*U2R*	*R2L*
FCM	68.7	71.3	80.1	62.6	49.3
FCM+RW	**69.2**	71.2	**82.2**	**63.4**	50.8
FCM+PR	69.1	**72.3**	80.4	59.6	**52.1**

Table II. FCM experimental results of 11 features (%)

Packet type	*Normal*	*Probe*	*DoS*	*U2R*	*R2L*
FCM	72.4	78.3	86.7	**57.6**	50.3
FCM+RW	**73.2**	77.9	87.2	54.4	50.8
FCM+PR	72.3	**79.2**	**87.4**	**57.6**	**52.1**

Table III. ECM experimental results of 24 features (%)

Packet type	*Normal*	*Probe*	*DoS*	*U2R*	*R2L*
FCM	76.4	74.5	85.6	42.1	53.1
FCM+RW	**76.8**	74.2	**86.2**	**44.5**	53.8
FCM+PR	**76.8**	**74.8**	85.6	42.1	**54.3**

Table IV. BPN experimental results of 9 features (%)

Packet type	*Normal*	*Probe*	*DoS*	*U2R*	*R2L*
FCM	85.2	88.6	94.6	66.8	72.5
FCM+RW	**85.8**	**89.1**	94.2	**67.9**	73.3
FCM+PR	85.5	88.3	**95.3**	66.5	**73.7**

Table V. BPN experimental results of 11 features (%)

Packet type	*Normal*	*Probe*	*DoS*	*U2R*	*R2L*
FCM	88.9	**92.5**	97.6	**66.8**	**72.5**
FCM+RW	**91.2**	90.1	**98.2**	63.1	70.3
FCM+PR	90.5	91.3	97.2	66.2	71.6

Table VI. BPN experimental results of 24 features (%)

Packet type	*Normal*	*Probe*	*DoS*	*U2R*	*R2L*
FCM	94.6	**98.0**	**99.9**	53.1	70.3
FCM+RW	**95.3**	96.4	**99.9**	55.3	**73.5**
FCM+PR	94.3	96.8	99.8	**58.6**	71.6

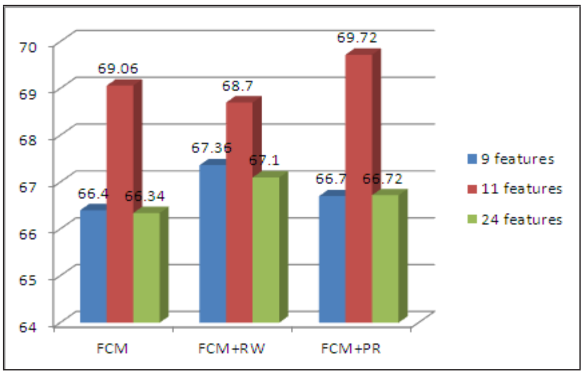

Fig. 2: Average detection rates-FCM (%)

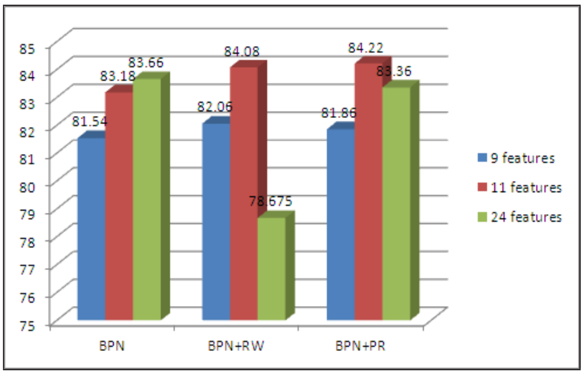

Fig. 3: Average detection rates-BPN (%)

Tables I-III demonstrate that the roulette wheel (RW) selection combined with the FCM scheme provides a higher detection rate for DoS and U2R attack packets; meanwhile, FCM with the pseudo-random (PR) rule can yield a higher detection rate for R2L and Probe attack packets when the 9 and 24 packet features are used. Additionally, the PR rule improves the detection rate for Probe, DoS, U2R and R2L packets when packet features are reduced to 11 features. It should be noticed that the biggest issue is misclassifying U2R and R2L connections as normal connections. Simulation results demonstrate that the proposed intrusion detection criteria applied in BPN can yield higher detection rates for the most expensive misclassification U2R (67.9%) and R2L (73.7%) connections as displayed in Tables IV and VI.

Moreover, the average detection rates of applying the PR rule into FCM and BPN can yield 69.72% and 84.22% when using 11 packet features; 84.22% and 83.36% detection rates are achieved by using the PR rule when using 24 features as indicated in Figures 2 and 3. Comparisons with other schemes are demonstrates in Figure 4; SVM denotes the self-organizing map neural networks applied based on 41 features [13], SOM indicates a linear support vector machine method based on 21 features [14]; ANN represents an artificial neural network based scheme was applied [15] which used 41 features for testing; conventional BPN with 24 features and the best performance schemes proposed in this work with 11 features involved. The proposed scheme, integrating the pseudo-random selection rule into BPN, outperforms other schemes.

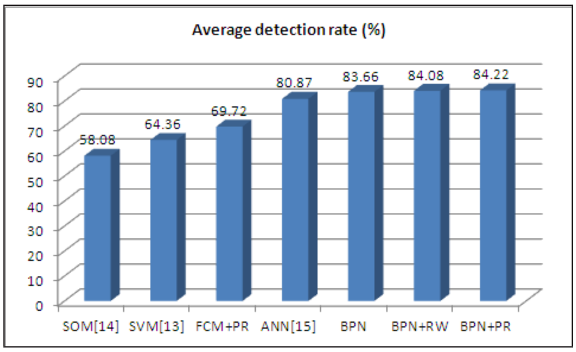

Fig. 4: Comparisons among different schemes

4 Conclusions

According to simulation results as displayed in Tables I, II and III, the average detection rates of proposed FCM and BPN integrating roulette wheel selection and FCM and BPN combining the pseudo-random rule are superior to the conventional competitive FCM and BPN. Hence, the proposed decision criteria combined with both clustering schemes are effective and efficient for abnormal packet detection. Meanwhile, pseudo-random rule integrated with FCM is able to improve the detection rate for anomaly detection (including Probe, DoS, U2R and R2L packets) when 11 packet features are used. Moreover, the average detection rate of using FCM integrating PR rule is higher than that of applying FCM combining RW when 11 features are involved; the detection performance of FCM involving RW selection rule is better than FCM involving the PR rule when 24 features are used. Curiously, for Probe, DoS and U2R intrusion packets, the detection performance of using 24 features is worse than that of using 11 features. Restated, more packet features used for intrusion identification does not guarantee higher detection rates. The reason behind this effect is that too many applied features may become noise and interfere in the clustering decision. The suggested scheme includes the pseudo-random rule in BPN which is able to provide higher average intrusion detection rate due to the proposed pseudo-random rule which enhances the intensification search. Meanwhile, only 11 features are required for intrusion detection (BPN+PR), further reducing the complexity and therefore computation time. However, a wide range of Internet applications are being developed. Hence, we have to face newly issued network attacks and intrusions. How to effectively detect these attacks with a high detection rate and low false positive rate to maintain a secure network environment is an important issue. Further investigation should focus on more efficient clustering methodology, especially for rare U2R and R2L intrusion connections.

Acknowledgement

This work was partly supported by the National Science Council, Taiwan, under contract NSC 99-2221-E-167-007

References

[1] A Fuchsberger, Intrusion Detection Systems and Intrusion Prevention Systems, Information Security Technical Report, **10**, 134-139, (2005).

[2] O. Depren, M. Topallar, E. Anarim and M.K. Ciliz, An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks, Expert Systems with Applications, **29**, 713-722 (2005).

[3] L. Khan, M. Awad and B. Thuraisingham, A new intrusion detection system using support vector machines and hierarchical clustering, The VLDB Journal, **16**, 507-521 (2007).

[4] S. Patton, W. Yurcik, and D. Doss, An Achilles Heel in Signature-Based IDS: Squealing False Positives in SNORT, Proc. Recent Advances in Intrusion Detection 2001 (RAID 2001), Davis, CA, October (2001).

[5] R. M. Chen and K.T. Hsieh, Effective Allied Network Security System Based on Designed Scheme with Conditional Legitimate Probability against Distributed Network Attacks and Intrusions, International Journal of Communication Systems, on-line June (2011).

[6] D. Song, M. I. Heywood, and A. N. Zincir-Heywood, Training Genetic Programming on Half a Million Patterns: An Example from Anomaly Detection, IEEE Transactions on Evolutionary Computation, **9**, 225-239 (2005).

[7] G. Poojitha, K. N. Kumar and P. J. Reddy, Intrusion Detection using Artificial Neural Network, Proc. 2010 International Conference on Computing Communication and Networking Technologies (ICCCNT 10), July, 1-7 (2010).

[8] W. Jiang, M. Yao and J. Yan, Intrusion Detection Based on Improved Fuzzy C-means Algorithm, Proc. International Symposium on Information Science and Engineering (ISISE 08), 326-329 (2008).

[9] L. A. Zadeh, Fuzzy sets, Information and Control, **8**, 338-353 (1965).
[10] J. C. Bezdek, Pattern Recognition with Fuzzy Objective Function Algorithms, New York: Plenum Press, (1981).
[11] M. Dorigo and L.M. Gambardella, Ant colony system: A cooperative learning approach to the traveling salesman problem, IEEE Transactions on Evolutionary Computation, **1**, 53-66 (1997).
[12] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[13] C. Fortuna, B. Fortuna and M. Mohorcic, Anomaly detection in computer networks using linear SVMs, Proc. Conference on Data Mining and Data Warehouses, Ljubljana, Slovenia, (2007).
[14] D. Jiang, Y. Yang and M. Xia, Research on Intrusion Detection Based on an Improved SOM Neural Network, Proc. International conference on Information Assurance and Security (IAS 09), 400-403 (2009).
[15] G. Poojitha,K.N. Kumar, P.J. Reddy, Intrusion Detection using Artificial Neural Network, Proc. 2010 International Conference on Computing Communication and Networking Technologies (ICCCNT), Karur, 1-7 (2010).

Ruey-Maw Chen received the B. S., the M. S. and the PhD degrees in engineering science from National Cheng Kung University of Taiwan R.O.C. in 1983, 1985 and 2000, respectively. From 1985 to 1994 he was a senior engineer on avionics system design at Chung Shan Institute of Science and Technology (CSIST). He was a networking engineer at Chinyi Institute of Technology during 1994 to 2002. Since 2002, he has been with the Department of Computer Science and Information Engineering, National Chinyi University of Technology (NCUT), where he is an associate professor. His research interests include meta-heuristics, scheduling optimization with applications and computer networks.