Clustering and Detecting Network Intrusion Based on Fuzzy Algorithms

Manar Y. Kashmola
Bayda I. Khaleel
College of Computer Sciences and Mathematics
University of Mosul

Received on: 29/06/2011
Accepted on: 02/11/2011

ABSTRACT

Clustering or (cluster analysis ) has been widely used in data analysis and pattern recognition. There are several algorithms for clustering large data sets or streaming data sets, Their aims to organize a collection of data items into clusters. These such items are more similar to each other within cluster, and difference than they are in the other clusters. Three fuzzy clustering algorithms (Fuzzy C-Means, Possibilistic C-Means and Gustafson-Kessel algorithms) were applied using kdd cup 99 data set to classify this data set into 23 classes according to the subtype of attacks. The same data set were classified into 5 classes according to the type of attacks. In order to evaluate the performance of the system, we compute the classification rate, detection rate and false alarm rate on this data set. Finally, the results obtained from the experiments with classification rate 100% which has not been obtained in any previous work.

Keyword: Network intrusion detection, Fuzzy C-Means(FCM), Possibilistic C-Means(PCM) and Gustafson-Kessel (GK) algorithms, kdd cup 99 data set.

الملخص

العنقدة (تحليل العنقود) تستخدم بشكل واسع في تحليل البيانات وتمييز الأنماط. هناك خوارزميات عديدة لـأبعاد أكثر كشمالية، كلية علوم الحاسبات والرياضيات، جامعة الموصل

تاريخ قبول البحث: 11/02/2011

1- Introduction

An intrusion detection system (IDS) is a component of the information security framework. Its main goal is to differentiate between normal activities of the system and behavior that can be classified as suspicious or intrusive. The goal of intrusion detection is to build a system which would automatically scan network activity and detect such intrusion attacks. Once an attack is detected, the system administrator can be informed who can take appropriate action to deal with the intrusion [12]. Intrusion detection techniques can be categorized into misuse detection and anomaly detection.
misuse detection uses the patterns of well-known attacks or vulnerable spots in the system to identify intrusions [4]. Misuse detection is based on the knowledge of system vulnerabilities and known attack patterns. Misuse detection is concerned with finding intruders who are attempting to break into a system by exploiting some known vulnerability, ideally, a system security administrator should be aware of all the known vulnerabilities and eliminate them [3].

- Anomaly detection attempts to determine whether can be flagged as intrusions. There are three types of intrusion detection systems: Host-based Intrusion Detection System (HIDS), Network-based Intrusion Detection System (NIDS), and combination of both types (Hybrid Intrusion Detection System). HIDS usually observes log or system –call on a single host, A host –based intrusion detection system places its reference monitor in the kernel / user layer and watches for anomalies in the system call patterns. While a NIDS typically monitors traffic flows and network packets on network segment, and thus observes multiple hosts simultaneously, NIDS performs traffic analysis on a local area network [12][4].

This research is organized as follows: in section 2 previous work 3 fuzzy clustering algorithms are discussed, section 4 (Knowledge Discovery and Data Mining) kdd data set used in this research, section 5 Data preprocessing, section 6 describes about the experiments and results obtained, and section 7 is conclusions.

2- Previous Work

In particular several clustering algorithms based approaches were employed for intrusion detection. Jawhar and Mehrotra [7] used fuzzy c-means clustering to classified dataset into 2 classes, they used (22133)records, the classification result in training stage is 99.9. Siddiqui[14] used parallel backpropagation neural network and parallel fuzzy ARTMAP, the detection rate result for parallel BP in the training stage is 98.36 and the detection rate in the testing stage is 81.73 and false alarm is 1.28. Detection rate for parallel fuzzy ARTMAP in training stage is 80.14 and in testing state detection rate is 80.52 and false alarm is 19.48.

3- Fuzzy Clustering Algorithms

3-1 Fuzzy C-Means Algorithm

The Fuzzy C-Means algorithm (FCM) is introduced by Bezdek [12]. Fuzzy c-means is based on Euclidean distance function [9]. It is a data clustering technique where each data point belongs to a cluster to some degree that is specified by membership grade [18]. Let X={x₁,x₂,…xₙ} be the set of n objects and V= {v₁,v₂,…vₖ} be the set of c centroids where xᵢ ∈ Rⁿ, vᵢ ∈ Rⁿ, and vᵢ ∈ X [10]. It partitions X into c clusters by minimizing the objective function :

\[ J_m(\mu, v) = \sum_{k=1}^{N} \sum_{i=1}^{c} (\mu_{ik})^m d_{ik}(x_i, v) \tag{1} \]

where \( d_{ik} \) is given by \( ||x_i - v_k|| \), c is the number of clusters in X, m is a weighting exponent [6]. The cluster centers are then evaluated by using the following equation:

\[ v_k = \frac{\sum_{i=1}^{N} (\mu_{ik})^m x_i}{\sum_{i=1}^{N} (\mu_{ik})^m} \tag{2} \]

and membership matrix \( \mu \) is update by the following equation:
\[ \mu_{ki} = \left[ \sum_{j=1}^{c} \left( \frac{d_{ki}}{d_{kj}} \right)^{\frac{2}{m-1}} \right]^{-1} \]  

…(3)

The parameter \( m \) is a weighting exponent on each fuzzy membership and determines the amount of fuzziness of resulting classification [13]. And membership value to the data items for the clusters within a range 0 and 1 [16].

3-2 Possibilistic C-Means Algorithm

(PCM) algorithm proposed by krishnapuram and keller [11]. Is based on a modification of the objective function of (FCM). The objective function is:

\[
\min \left\{ J_m(x, \mu, c) = \sum_{i=1}^{c} \sum_{j=1}^{N} \mu_{ij}^m d_{ij}^2 + \sum_{i=1}^{c} \eta_i \sum_{j=1}^{N} (1 - \mu_{ij})^m \right\} \]

…(4)

and the membership is updated the following equation:

\[
\mu_{ij} = \frac{1}{1 + \left( \frac{d_{ij}^2}{\eta_i} \right)^{m-1}} \]

…(5)

Where \( \eta_i \) is the suitable positive number [8].

3-3 Gustafson-Kessel Algorithm

The Gustafson-kessel (GK) is the extension of the fuzzy c-means algorithm. The objective function is:

\[
J_q(S, \mu, V) = \sum_{j=1}^{c} \sum_{i=1}^{n} \left( \mu_{ij} \right)^q D_{ij}^2 \]

…(6)

Where \( c \) and \( n \) are the number of clusters and data respectively, \( \mu \) is a set of membership values \( \mu_{ij} \), \( V \) is a vector containing the values of clusters \( v_i \), \( q \) is the fuzzifier and \( D_{ij} \) is the distance. GK used mahalanobis distance.

\[
D_{ij}^2 = (S_j - v_i)^T A_j (S_j - v_i) \]

…(7)

The \( A_j \) is calculated from the following equation:

\[
A_j = \left[ \rho_i \det(F_i) \right]^{\frac{1}{n}} F_i^{-1} \]

…(8)

And \( F_i \) is calculated as follows:

\[
F_i = \sum_{j=1}^{n} \left( \mu_{ij} \right)^q (S_j - v_i) (S_j - v_i)^T \sum_{j=1}^{n} \left( \mu_{ij} \right)^q \]

…(9)

Where \( F_i \) is the fuzzy covariance matrix and \( \rho_i \) the cluster volume which is usually set to 1 [1].

4- Kdd Dataset

(Knowledge Discovery and Data Mining) KDD’99 has been the most widely used data set. The network data is distributed by MIT Lincoln Lab for Defense Advanced Research Projects Agency DARPA The KDD cup 99 dataset includes a set of
41 features derived for each connection and a label which specifies the status of connection records as either normal or specific attack type. These features had all forms of continuous, discrete, and symbolic. The data set encompasses different attack types grouped into one of four categories [17]:

- Dos (Denial Of Service): making some computing or memory resources too busy so that deny legitimate users access to these.
- Probe: Host and port scans as precursors to other attacks. An a network to gather information or find known vulnerabilities, e.g., portsweep.
- U2R (User to Root): Unauthorized access to local super user (root) privileges using system's susceptibility, e.g., buffer_overflow.
- R2L (Remote to Local): Unauthorized access from a remote machine according to exploit machine's vulnerabilities, e.g., imap.

Total number of connection records in training data set is 10% data (494020) records. And the total number of connection record in testing data set is corrected file (311029) records. Table (1) shows the data set used in training and testing stages that contain from normal and attack connection records [17][2].

Table (1) is described the number of samples kdd data set that used [17]

| Data set       | Normal | Dos  | Probe | U2R  | R2L  | Total |
|----------------|--------|------|-------|------|------|-------|
| Corrected kdd  | 60593  | 229853 | 4166  | 70   | 16347 | 311029 |
| 10_precent kdd | 97277  | 391458 | 4107  | 52   | 1126  | 494020 |

5- Data Preprocessing

Data training and testing was taken from (DARPA). This data consist of symbolic and numeric values, all symbolic values were transformed into numeric values [15]. In this research kdd dataset (10_precent kdd) are used in the training stage and (corrected kdd) in the testing stage which contains 41 features (numeric and symbolic), in this research each symbolic of features such as three types of protocols (tcp, udp, icmp) and 68 type of services and 11 types of flag, takes value from [1..n] and then normalized all input data of 10%kdd data set.

6- Experiments And Results

Two indicators were used to measure the accuracy of the methods: detection rate and false alarm rate. The detection rate (DR) shows the percentage of true intrusions that have been successfully detected. While the false alarm rate is defined as the number of normal instances incorrectly labeled as intrusion by the total number of normal instances [4].

6-1 Experiment 1

- First stage, we applied three fuzzy clustering algorithms FCM, PCM, and GK to 10%kdd data set that contains (494020) records. In the first experiment, we apply these three fuzzy clustering algorithms to classify this data set into 23 classes or clusters, One for normal and the rest classes for the types of attacks { DoS (pod, land, back, Neptune, teardrop, smurf), probe (ipsweep, portsweep, satan, nmap), U2R (buffer _overflow, loadmodule, perl, rootkit), R2L(ftp_write, guess_passwd, imap, multihop, phf, spy, Warezclient, warezmater )}. Table(2) shows the result clustering after training these three fuzzy clustering algorithms. The results of classification rate obtained is 100% to classify data into 23 classes one class for normal behavior and 22
classes for different types of attacks, but these three fuzzy algorithms took different iterations and different times. (When used HP laptop, Intel(R) core (TM) i3 CPU 2.27 GHZ, and RAM 2 GB).

Table (2). The clustering result after training three fuzzy clustering algorithms FCM, GK, PCM to classify data set into 23 clusters

| Amount | Sub type of attack | Samples rate |
|--------|-------------------|--------------|
| 4      | phf               | 0.000810     |
| 107201 | neptune           | 21.699729    |
| 3      | perl              | 0.000607     |
| 9      | loadmodule        | 0.001822     |
| 1020   | warezclient       | 0.206469     |
| 231    | nmap              | 0.046759     |
| 97277  | normal            | 19.690903    |
| 2203   | back              | 0.445933     |
| 8      | ftp_write         | 0.001619     |
| 21     | land              | 0.004251     |
| 264    | pod               | 0.053439     |
| 280790 | smurf             | 56.837780    |
| 1247   | ipsweep           | 0.252419     |
| 30     | buffer_overflow   | 0.006073     |
| 7      | multihop          | 0.001417     |
| 2      | spy               | 0.000405     |
| 1589   | satan             | 0.321647     |
| 979    | teardrop          | 0.198170     |
| 20     | warezmaster       | 0.004048     |
| 12     | imap              | 0.002429     |
| 1040   | portsweep         | 0.210518     |
| 10     | rootkit           | 0.002024     |
| 53     | guess_passwd      | 0.010728     |

Table (3) shows the result of the first experiment that using FCM, PCM and GK clustering about 23 classes. Whereas Figure (1) shows the relationship between these algorithms and iterations number while Figure (2) shows the relationship between algorithms and time for 23 classes.

As shown in table (3) PCM was classified data set faster than other two algorithms, because PCM takes a number of iterations and time less than other algorithms, but FCM takes a number of iteration greater than GK and PCM algorithms.

The classification rate[5] about three fuzzy clustering algorithms was calculated by equation (10):

\[
classification\ rate = \frac{\text{number of classified patterns}}{\text{total number of patterns}} \times 100
\]  

\(\text{...(10)}\)
Table (3). The result of the FCM, GK, PCM clustering

| Type of Clustering algorithms | Fuzzification member | Iteration number | Time second | Classification rate |
|-------------------------------|---------------------|------------------|-------------|---------------------|
| FCM                           | 1.2                 | 27               | 583.8       | 100%                |
| GK                            | 1.2                 | 17               | 775.4       | 100%                |
| PCM                           | 1.2                 | 14               | 307.5       | 100%                |

- Second stage: “corrected KDD file” data set that contains (311029) records were used in the testing stage on the three fuzzy clustering algorithms FCM, GK, and PCM. Table (4) shows the results of the testing “corrected KDD “ file in FCM with detection rate for each attack and normal.

Table (4). results of testing stage of FCM Algorithm

| Type   | Sub Type | No. of input attacks | No. of detected attacks | DR    |
|--------|----------|----------------------|-------------------------|-------|
| Normal |          |                      |                         |       |
|      |          | 60593                | 34664                   | 57.208|
| Dos    | apache2  | 794                  | 794                     | 100%  |
| Dos    | pod      | 87                   | 87                      | 100%  |
| Dos    | smurf    | 164091               | 164078                  | 99.991|
| Dos    | back     | 1098                 | 1098                    | 100%  |
| Dos    | land     | 9                    | 9                       | 100%  |
| Dos    | mailbomb | 5000                 | 5000                    | 100%  |
| Dos    | neptune  | 58001                | 58001                   | 100%  |
| Dos    | process  | 759                  | 759                     | 100%  |
| Dos    | teardrop | 12                   | 0.0                     | 0.0   |
| Dos    | udpstorm | 2                    | 0.0                     | 0.0   |
| Probe  | ipsweep  | 306                  | 320                     | 95.625|
| Probe  | portswep | 354                  | 0.0                     | 0.0   |
| Probe  | saint    | 736                  | 1090                    | 67.523|
| Probe  | mscan    | 1053                 | 1053                    | 100%  |
Clustering and Detecting Network Intrusion Based on Fuzzy Algorithms

Table (5) shows the results of testing data by using GK algorithm with the detection rate for each attack and normal behavior.

| Type | Sub Type | No. of input attacks | No. of detected attacks | DR |
|------|----------|----------------------|-------------------------|----|
| Normal | | 60593 | 33418 | 55.152 |
| Dos | neptune | 58001 | 40372 | 69.606 |
| | smurf | 164091 | 131134 | 79.915 |
| Probe | ipsweep | 354 | 252 | 82.353 |
| U2R | | 70 | 0.0 | 0.0 |
| R2L | snmpgetattack | 7741 | 53043 | 14.594 |

Table (6) shows the results testing stage after applying PCM algorithm with the detection rate for each of attack and normal.

| Type | Sub Type | No. of input attacks | No. of detected attacks | DR |
|------|----------|----------------------|-------------------------|----|
| Normal | | 60593 | 61387 | 98.707 |
| Dos | pod | 87 | 85 | 97.701 |
| | smurf | 164091 | 164093 | 99.999 |
| | land | 9 | 1104 | 0.815 |
| | mailbomb | 5000 | 4902 | 98.040 |
| | neptune | 58001 | 40735 | 70.231 |
| | processtable | 759 | 357 | 47.299 |
| Probe | saint | 736 | 1398 | 52.647 |
| | satan | 1633 | 13212 | 12.364 |
| U2R | | 70 | 0.0 | 0.0 |
| R2L | snmpgetattack | 7741 | 5975 | 77.238 |

Finally, table (7) shows the comparisons between three fuzzy clustering algorithms FCM, GK and PCM for 23 classes with over all detection rate that obtained for FCM is equal to (91.659) and for GK is equal to (83.021) and detection rate for PCM is equal to (94.284).

Table (7), comparison between FCM, GK and PCM Clustering Algorithm

| Performance measure | FCM | GK | PCM |
|---------------------|-----|----|-----|
|                     |     |    |     |
Figures (3, 4, and 5) show the relationship between three clustering algorithms with (Detection rate – false alarm rate – time) respectively.

**Figure (3).** relationship between algorithms with Detection Rate  
**Figure (4).** relationship between algorithms with False Alarm Rate  
**Figure (5).** relationship between algorithms with time

### 6-2 Experiment 2

The same data set (494020) records were used after preprocessing it in the training stage to classify it into 5 classes, Table(8) shows the results of experiment for FCM, GK and PCM.

**Table (8).** The clustering results after training three fuzzy clustering algorithms FCM, GK, PCM to classify data set into 5 clusters
While table (9) shows the results after applying these three fuzzy clustering algorithms FCM, PCM, and GK to classify data set into 5 classes. As shown in table (9) PCM was classified data set faster than other two algorithms, because PCM takes a number of iterations and time less than other algorithms, but FCM take a number of iteration greater than GK and PCM algorithms.

**Table (9). result of the FCM, GK, PCM clustering**

| Type of Clustering algorithms | Fuzzification member | Iteration number | Time second | Classification rate |
|------------------------------|----------------------|------------------|-------------|---------------------|
| FCM                          | 1.011                | 26               | 134.7       | 100%                |
| GK                           | 1.011                | 16               | 144.5       | 100%                |
| PCM                          | 1.011                | 12               | 67.2        | 100%                |

- The second stage of this experiment “corrected KDD file” data set that consists of (311029) records also were used in the testing stage on three fuzzy clustering algorithms FCM, GK, and PCM. Table (10) shows the results of the testing “corrected KDD “ file in FCM with detection rate for each attack type and for normal. In which the normal behavior got the higher detection rate is equal (97.813).

**Table (10). results of testing stage of FCM Algorithm**

| Type | No. of input attacks | No. of detected attacks | DR     |
|------|----------------------|-------------------------|--------|
| Normal | 60593                | 61948                   | 97.813 |
| Dos   | 229853               | 164611                  | 71.616 |
| Probe | 4166                 | 44212                   | 9.428  |
| U2R   | 70                   | 0.0                     | 0.0    |
| R2L   | 16347                | 35795                   | 45.668 |

After testing data in GK algorithm, the higher detection rate obtained is (98.498) for normal behavior. Which are shown in table (11).

**Table (11). results of testing stage by using GK Algorithm**

| Type | No. of input attacks | No. of detected attacks | DR     |
|------|----------------------|-------------------------|--------|
| Normal | 60593                | 59683                   | 98.498 |
| Dos   | 229853               | 171158                  | 74.464 |
| Probe | 4166                 | 0.0                     | 0.0    |
| U2R   | 70                   | 0.0                     | 0.0    |
| R2L   | 16347                | 20583                   | 79.4199|

Using Possibilistic c-means (PCM), normal behavior got higher detection rate equals to (99.972) after the testing data set shown in table (12).
Table(12). show results of testing stage using PCM

| Type      | No. of input attacks | No. of detected attacks | DR       |
|-----------|----------------------|-------------------------|----------|
| Normal    | 60593                | 60523                   | 99.972   |
| Dos       | 229853               | 164145                  | 71.413   |
| Probe     | 4166                 | 0.0                     | 0.0      |
| U2R       | 70                   | 0.0                     | 0.0      |
| R2L       | 16347                | 86291                   | 18.944   |

Finally, table (13) shows the comparisons between three fuzzy clustering algorithms FCM, GK and PCM for 5 classes, with over all detection rate that obtained for FCM is equal to (98.543%) and false alarm equal to (2.236%), while the detection rate that obtained for GK is equal to (80.836%) and false alarm equal to (1.502%), and the detection rate that obtained for PCM is equal to (99.955%) and false alarm equal to (0.116%).

Table(13). comparison between FCM, GK and PCM Clustering Algorithms

| Performance measure       | FCM           | GK            | PCM           |
|---------------------------|---------------|---------------|---------------|
| Normal detection          | 61948         | 59683         | 60523         |
| Attack detection          | 244548        | 251424        | 250366        |
| Detection rate_normal     | 97.813        | 98.498        | 99.884        |
| Detection rate_attack     | 97.649        | 76.562        | 99.972        |
| False_alarm rate          | 2.236         | 1.502         | 0.116         |
| Detection_rate            | 98.543        | 80.836        | 99.955        |
| Times                     | 2.7 second    | 5.8 second    | 2.6 second    |
| Fuzzification member       | 1.011         | 1.011         | 1.011         |
| Iterations                | 1             | 1             | 1             |

Figures (6, 7, and 8) show the relationship between three clustering algorithms with (Detection rate –false alarm rate – time) respectively.

Figure(6). relationship between algorithms with Detection Rate

Figure(7). relationship between algorithms with False Alarm Rate
Finally, table (14) shows the comparisons results of the three fuzzy clustering algorithms FCM, GK and PCM with the previous work.

Table (14). comparison results of FCM, GK, PCM algorithms with previous work

| Algorithm type | Dataset          | Normal | Attack | Classification rate% | Detection rate |
|----------------|------------------|--------|--------|----------------------|----------------|
| FCM[7]         | Training (22133) | *      | *      | 99.9                 |                |
| Parallel fuzzy ART MAP [14] | Training set | *      | *      | *                   | 80.14          |
| Parallel fuzzy ART MAP [14] | Testing set | *      | *      | *                   | 80.52          |

**First experiment**

| Algorithm | Dataset          | Normal | Attack | Classification rate% | Detection rate |
|-----------|------------------|--------|--------|----------------------|----------------|
| FCM       | Training set     | 100    | 100    | 100                  |                |
| FCM       | Testing set      | 57.208 | 99.995 | 91.659               |                |
| GK        | Training set     | 100    | 100    | 100                  |                |
| GK        | Testing set      | 55.152 | 89.764 | 83.021               |                |
| PCM       | Training set     | 100    | 100    | 100                  |                |
| PCM       | Testing set      | 98.707 | 92.58  | 94.284               |                |

**Second experiment**

| Algorithm | Dataset          | Normal | Attack | Classification rate% | Detection rate |
|-----------|------------------|--------|--------|----------------------|----------------|
| FCM       | Training set     | 100    | 100    | 100                  |                |
| FCM       | Testing set      | 97.813 | 97.649 | 98.543               |                |
| GK        | Training set     | 100    | 100    | 100                  |                |
| GK        | Testing set      | 98.498 | 76.563 | 80.836               |                |
| PCM       | Training set     | 100    | 100    | 100                  |                |
| PCM       | Testing set      | 99.884 | 99.972 | 99.955               |                |
7- Conclusions

In this research, three fuzzy clustering algorithms were applied to classify intrusion into 23 classes and also classify the same data set into 5 classes. In the first experiment, these three fuzzy clustering algorithms classify 10% kdd data set into 23 classes, one for normal and others for subtypes of attacks and detect these attacks in the first stage of the first experiment by using the fuzzy clustering algorithms FCM, GK and PCM; the classification rate obtained is 100% for these three algorithms. And in the second stage of the first experiment we have got higher detection rate for (PCM) algorithm is equal to (94.284) and less false_alarm rate (1.310). While the (FCM) algorithm got detection rate is equal to (91.659) and false_alarm rate (42.792), and finally, (GK) algorithm got the smaller detection rate (83.021) and higher false_alarm rate (44.848).

In the second experiment, these three fuzzy clustering algorithms classify 10% kdd data set into 5 classes, one for normal and others for types of attacks and detect these attacks. In the first stage of the second experiment, we obtained 100% classification rate for the three fuzzy clustering algorithms FCM, GK and PCM, and in the second stage (PCM) algorithm got higher detection rate (99.955) and less false_alarm rate (0.116). While (FCM) algorithm got on (98.543), but it is got higher false_alarm rate (2.236) and finally, (GK) algorithm has got the smaller detection rate (80.836) and false_alarm rate (1.502). So the results PCM are best performance and next FCM and last GK.

After applying three clustering algorithms (FCM, GK, PCM) on the kdd 99 dataset obtained the following:

- When implement PCM algorithm on this dataset to classify it into 23,5 class, this algorithm got high classification rate (100%) in a few number of iteration and less time compared with the other algorithms.
- Also the PCM algorithm got high detection rate and low false alarm compared with the other algorithms.
REFERENCES

[1] Ali M., Karmakar G., Dooley L., "fuzzy clustering for image segmentation using generic shape information ", Malaysian journal of computer science, Vol.21(2). 2008.

[2] Betanzos A., Marono N., Fortes F., Romero J., Sanchez B., " Classification of computer intrusions using functional network. A comparative study ", European Symposium on Artificial Neural Networks Bruges(Belgium), 25-27 April 2007.

[3] Chebrolu S., Abraham A., Thomas J., " Feature deduction and ensemble design of intrusion detection system ", www.elsevier.com/locate/cose . 2004.

[4] Chimphlee W., Abdullah A., Sap M., Chimphlee S., Srinoy S., " A rough-fuzzy Hybrid Algorith for Computer Intrusion Detection ", the international Arab journal of information Technology, Vol.4, No.3, 2007.

[5] Faraoun K., Boukelif A., " Neural network learning improvement using the K-means clustering algorithm to detect network intrusions", www.waset.org/journals/waset/V34-86.pdf. International Journal of computational Intelligence 3;2.

[6] Gomathi M., Thangaraj P., "A New approach to lung image segmentation using fuzzy possibilistic c-means Algorithm ", international journal of computer science and information security, Vol.7, No.3, 2010.

[7] Jawhar M., Mehrotra M., "Design network intrusion detection system using hybrid fuzzy-neural network". www.csjournals.org/csc/ manuscript /journals/IJcss. International Journal of computer science and security, volume (4): issue(3).

[8] Kumar A., Ghosh S., Dadhwal V., "A comparison of the performance of fuzzy algorithm versus statistical algorithm based sub-pixel classifier remote sensing data ", www.isprs.org/proceedings/XXXVI/part 7/pdf/153.pdf .

[9] Liu H., Wu D., Yih J., Liu S., "fuzzy possibilistic c-means based on mahalanobis distance separable criterion ", WSEAS TRANSACTION ON BIOLOGY AND BIOMEDICINE, issue 7, volume 4, july 2007

[10] Maji P., Pal S., "rough set based generalized fuzzy c-means algorithm and quantitative indices ", IEEE, vol.37, no.6, 2007.

[11] Masulli F., Schenone A., "A fuzzy clustering based segmentation system as support to diagnosis in medical imaging ", ELSEVIER, 1999 Elsevier science B.V., Artificial intelligence in medicine 16 (1999) 129-147.

[12] Panda M., Patra M., "some clustering algorithms to enhance the performance of the network intrusion detection system ", journal of theoretical and applied information technology, pp.795-801, 2008.

[13] Saad M., Alimi A., " Modified fuzzy possibilistic c-means ", proceeding of the international MultiCoference of Engineers and Computer Scientists Vol I, 2009.

[14] Siddiqui M., "high performance data mining techniques for intrusion detection ", thesis 2004.
[15] Siripanwattana W., Srinoy S., " information security based on soft computing techniques ", Proceeding of the International MultiConference of Engineers and Computer Scientists Vol I. 2008.

[16] Thomas B., Raju G., Wangmo S., " A modified fuzzy c-means algorithm for natural data exploration ", World Academy of science, Engineering and technology 49, 2009.

[17] Toosi A., Kahani M., Monsefi R., " network intrusion detection based on neuro-fuzzy classification ", IEEE 2006.

[18] Vlad Z., Ofelia M., Maria T., "fuzzy clustering in an intelligent Agent for diagnosis establishment ", scientific Bulletin of the petru maior university of tigumures, vol.6(XXIII), ISSN 1841-9267, i.e inter-eng, 2009.