Optimization of Intrusion Detection Systems to increase the efficiency using artificial neural networks

Mahyar Najizad[1], Mahmoud Najizad[2]
[1]Software engineer, Najizad1373@gmail.com Phone:+989301649865
[2]power Engineer, Email:mnadjizad@gmail.com

Summary
The intrusion detection system is a tool that tries to uncover intrusions and collect evidence of intrusions to repair data and modify system behavior. There are three methods for intrusion detection: detection of abuse, anomaly detection, and detection combined of these two factors with each other. The relationship between different networks and the variety of users has led to major issues such as theft, destruction and manipulation of information. For this purpose, systems known as Intrusion Detection Systems have been developed to identify suspicious behaviors, which today, in computer networks, these systems are used as a defensive tool against attacks and in order to protect information. The main purpose of this paper is to use artificial neural network system to detect intrusions, and also the error percentage of each of the two methods stated in this study is evaluated. Finally, a good solution is suggested to increase the security of the system.

Key words
Intrusion detection systems, Artificial Neural Networks, Intrusion Detection, Inspection

1. Introduction

Information is considered as one of the most important assets of organizations. Organizations consider their dependence on information based on processing and everyday use of it. Increasing use of e-commerce has already been caused advent of information security protection. The confidentiality of information, the integrity of information and the secure presence of information are one of the biggest concerns in the field of computer networks. Intrusion detection system is capable of detecting, preventing and even reacting to security attacks. Today, it is considered an integral part of information security, but it is worth noting that there is no system technically to create without any vulnerability. Here, this intrusion detection system can be a good topic for research and development. According to a recent report, the threat of computer systems in the past five years has increased, resulting in a loss of $ 100 billion. Since the 1970s when the issue of intrusion detection systems has been raised, many studies have been conducted in this field, and the need for security systems has grown a lot [1]. In 1977, 1978, the International Standard Organization convened a meeting between governments and Electronic Data Processing (EDP) inspection bodies, resulting in a report on security, inspection and control of systems at that time. At the same time, the US Department of Energy began a very detailed investigation into the inspection and security of computer systems due to concerns about the security of its systems. This work was done by a person named James P. Anderson [2]. Anderson is the first person who presented an article on the need for automated inspection of system security. The report, produced in 1980, can be introduced as the core of the concept of intrusion detection. In this report, mechanisms are introduce for system security inspections, and it is also cleared how to deal with it in the event of a system failure. From 1984 to 1986, Peter Neumann and Dorotty Denning conducted research on the security of computer systems, which resulted in the production of a real-time intrusion detection system operating on the basis of expert systems. This system was named IDES. In this project, a combination of anomaly detection and abuse detection was studied. The idea presented in this project was used as the basis for many of the intrusion detection systems that were developed since then [3]. Anderson's report and research on the IDES project were the start of a series of investigations into intrusion detection systems. In "Intrusion Detection using the *Gaussian* mixture *model* and Comparison and Composition with Backup Vector Machine", we attempt to detect intrusion using the Gaussian mixture Model and support vector machine.

Since the error areas of these two methods are not necessarily complete overlap, the optimal combination of these two methods has been used to reduce the error rate and increase the efficiency of intrusion detection. In this project, Gaussian mixture model techniques and Backup Vector Machine are used to determine the intrusion type from the KDD-99 database to evaluate them. The extracted features of the data include personalized communication features, timed traffic features, and a number of semantic features. A total of 41 features are extracted from the data. The data in this database is in one of the DOS, R2L, U2R, Noral, and Probe categories [4]. Feature selection is one of the problems of intrusion detection systems. In the tests of intrusion detection

Manuscript received October 5, 2017
Manuscript revised October 20, 2017

systems using the Gaussian mixture model, the efficiency of various features has been investigated. The use of features that is obtained from data transmitted through each connection is effective in detecting U2R, R2L, DOS, and Normal status. This technique has a higher generalizability and is able to detect unknown attacks, however since the error areas of these two methods necessarily do not necessarily overlap, they have a high error rate [5]. Further, in other studies, a partial use of the Inspector for Intrusion Detection Systems has been explored for study on proper function of Intrusion Detection Systems by Mobile Agents. For the inspector, three general architectures have been suggested, which they are called the local inspector, the central inspector and the mobile inspector. Then, these three inspector architectures are compared in terms of response time, network load, and system load. In addition to these cases, another criterion is considered as the function of re-configuration of the system and the results of the experiments have shown that the performance of the local inspector compared to two other samples has less response time and less load.

This conclusion suggests that the use of local inspectors in small networks is appropriate [6]. In this research, intrusion detection is done using artificial neural network methods. In this method, they can be used in intrusion detection systems due to the ability to have high classification and generalization power. The sample network uses three levels of hierarchy, which each low-level intrusion detection system sends a report to the high-level intrusion detection system. The intrusion detection system extracts network connectivity features by receiving packets from the network and, after pre-processing statistics on connections, detects unusual behaviors at the network level using neural network classes.

2. Intrusion detection systems

In the network intrusion issue, the Intruder essentially tries to close its unauthorized activity to the system's authorized behaviors so that it cannot be identified, which makes it more difficult to detect anomaly. Because there is always the intrusion and abuse of computer systems and networks, and making empty systems of forms is something very difficult or impossible, there is a need to take steps to deal with such abuses. For this reason, today there are many efforts to provide methods of detection and coping with intrusion [7]. With the advancement of technology, as the manner of intrusive activities has changed, expectations from intrusion detection systems have also increased [8]. An important category of intrusion detection systems uses learning methods to model intrusion. An intrusion detection system is one or more systems that can detect changes and behaviors in a host or network. In this section, a brief description of the general concepts of intrusion detection systems is described [9-10].

Architecture of intrusion detection systems

• Information collector section

This section is responsible for collecting information. For example, this section should be able to detect changes in the system file or network performance and collect the necessary information.

• System Verification section

Each intrusion detection system should have a section that evaluates the system itself in terms of performance. In this way, you can ensure the correct operation of the system.

• Information storage section

Each intrusion detection system stores its information in a location. This location can be a simple text file or a database.

• The control and management section

By this section, the user can communicate with the intrusion detection system and give it the necessary commands.

• Analysis section

This section of the Intrusion Detection System is responsible for reviewing the collected data.

Intrusion and intrusion Factors

Intrusion is a collection of illegal actions that compromise the integrity, confidentiality, or access to a resource. In general, intrusion can be divided into the following categories:

• Illegal Login: It happens when an alien accesses the user ID and password.

• Deceptive attacks occur when the attacker persuades the system that he is a legitimate user.

• Access to the security control system: The attacker tries to correct system security issues.

• Leakage: when information is transmitted to the outside of the system.

• Preventing Service Provision: It's when the sources are unavailable for other users.

• Misuse: includes attacks such as file deletion and resource abuse

3. Artificial Neural Networks

The network is a multi-layer perceptron network, which is a network of Feed-Forward networks. In this kind of networks, information goes only one side forward (through the input layer to the hidden layer and through the hidden layer to the output layer). The learning algorithm of this network is an error propagation type and the type of stimulation function is also the Sigmoe Tangent [11]. Neural networks consist of a series of layers consisting of simple components called neurons that act in parallel. In Figure 1, a simple neuron with input R is shown that each input vector is weighed by the proper

choice of weight W and the sum of Bias inputs develops the input of the moving function.

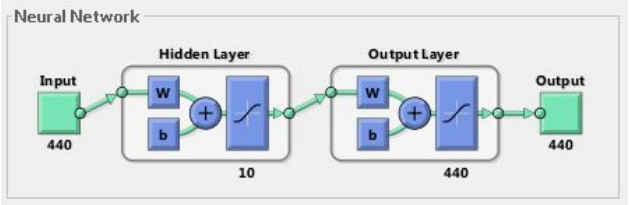

Figure 1: Two-layer feed-forward neuron network model

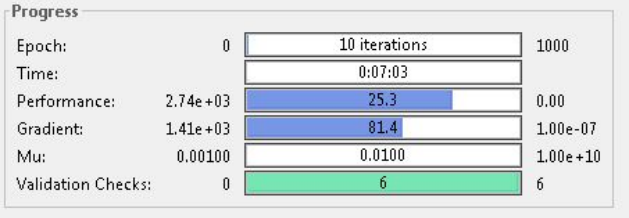

Figure 2: Two-layer feed-forward neuron network analysis

The most important point in the neural networks is to normalize the input parameters obtained through (1). If we consider the input parameters in this system as a signal, then we can claim that the behavior of this signal at time t can depend on the behavior of the signal at time t-1. The input parameters to the network are entered to multi-layer perceptron neural network based on all commonly used methods and 70% of the data for the training phase, 70% for the test phase and 10% for the validation phase have been selected. 440 cases have been considered for input data[12].

$$x' = \frac{x_i - x_{min}}{x_{max} - x_{min}} \qquad (1)$$

In this equation, x_i is the input parameter, x_{min} is the minimum value of parameter x, x_{max} is the maximum value of parameter x, x' is the parameter's normalized value x_i. The error detection and predictive indicators used in this study are as follows. With regard to how each section of an intrusion detection system is located, different architectures are created for it. In terms of the architecture of intrusion detection systems, there is another viewpoint that from this point of view, two general architectures can be considered:

• The system under protection and intrusion detection system are in one location.

• The system under protection and intrusion detection system are placed separately.

Separating the intrusion detection system from the protected system has some advantages:

• Prevent erasure of records stored by the intrusion detection system. •

• Preventing change of information from attacker

• Enhance performance by reducing the processing load on a protected system.

4. The squared mean squared error value a criterion for obtaining the best estimate

RMSE value is determined based on mean squared error[13].

$$RMSE = \frac{\sum_{i=1}^{n}(y_{est} - y_{act})^2}{n} \qquad (2)$$

When the network parameters are obtained after a complete period of patterns presentation, in the phrase epoxy or a cycle is called to this type of repetition; the number of network replicators is equal to the number of learning data. The effect of various combinations of input variables on the error value is the last evaluation of the compiled models. By performing sensitivity analysis for each neural network model, irrelevant input data can be identified and deleted. Removing these data reduces the cost of data collection and in most cases increases the accuracy of the model. The sensitivity analysis based on the average ratio for compiled models has been expressed in the artificial intelligence neural network algorithm. In the feed-forward back propagation network, firstly, the weights of the output layer are adjusted, since for each of the external layer neurons there is a desired amount that can modulate the weights. After calculating the training error by the network, its value is compared with the desired value and the training error is calculated and the learning algorithm attempts to optimize the error value associated with it. If the training error is less than the predetermined error, the learning process will end. In the training phase, firstly the computation begins from the input of the network to its output, and then the calculated error values are propagated to the previous layers.

Initially, the output volume is performed as a layer in the layer and the output of each layer will be input of next layer. The structure of a neural network is determined by determining the number of layers, the number of neurons in each layer, the stimulus function (output controller of each neuron), the training method, the weight correction algorithm, and the type of model. The 5-layer nerve-fuzzy comparative inference system consists of nodes and knot arrows. The first layer is the input data with the degree of membership that is specified by the user. All modeling operations are done in layers 2 - 4. The last layer is the output of the network, which aims to minimize the difference between the output from the network and the real output.

5. Analytical methods

In the process of intrusion detection after the introduction of information sources and the categorization of them, it is necessary to determine the next analyzer. In the data analyst, information is extracted from the information sources, and according to security policies, types of attacks, etc. are examined [1-3]. In intrusion detection systems, analysis methods are divided into two general categories of abuse detection, anomaly detection and/or a combination of them:

Abuse Detection

In this method, the analyzer looks for a sign that represents an opposite action. To do this, first information is filtered to find patterns that indicate the type of attack or other security policies. In abuse Detection, this work is done by pattern recognition mechanisms. Currently, most intrusion detection systems use this method [16].

6. Anomaly diagnosis

In this method, the analyst looks for unusual cases. To do this, the collected information is examined to find patterns that represent unusual actions. In some cases, these two methods are used together. In these systems, an anomaly detection procedure has the task of detecting new and unknown attacks and abuse detection has the task of protecting the anomaly detection system. By doing so, it ensures that the collected information and patterns are safe for the anomaly detection system. In Figure 1, a diagram of a system that uses two methods is displayed.

Intrusion detection methods to computer networks

7. Abnormal behavior detection

In order to detect abnormal behavior, one can first visualize the behaviors of each user, then compare the current behavior of users with these views, and, in the event of any inconsistency, informs the system security officer about abnormal behavior [2]. Users' behavioral views are defined as a set of measurable metrics. These criteria are private aspects of users' behavior.

In general, daily use of users follows a computer system of recognizable behavior patterns.

8. Abuse Detection

The main idea in detecting abuse is that there are ways in which any intrusion can be displayed in the form of a pattern so that different types of the same intrusion can be identified. This issue can achieve a high level of accuracy due to the simple range of topics that are modeled.

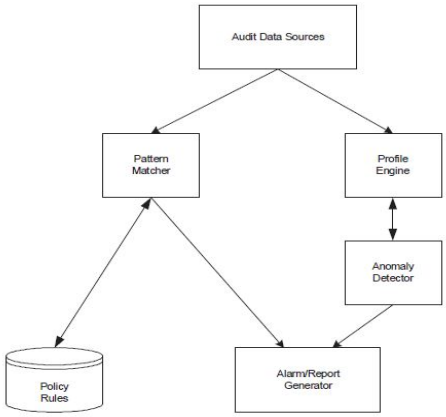

Fig 3. Structure of an intrusion detection system

9. Control of system

Another problem with intrusion detection systems is the system control problem. To do this, three major methods are used.

9.1. Central

In this model, the management and reporting system is centralized. In this method, a central management system controls the intrusion detection system [16].

The use of this method is a prerequisite, for example, the exchange of information between the center and other sectors should be carried out safely. In addition to this, there should be a way to determine what part of the system is in operation at any given moment and what part of the move is stopped. Another issue in relation to the central model is the final conditional submission to the end users.

10. Use of network management facilities

In order to solve the problems that the central method has, the intrusion detection function can be implemented as a function of the network management system [14]. In this way, the collected information by network management systems can be used as a source of information for intrusion detection systems.

10.1. Distributed

Another way to solve the central state problem is to use the distributed model. In this case, the analyzer is not central. The method that can be used in this model is to use mobile agents. In this case, the analyzer moves at the network level and analyzes the results gathered on different systems.

11. Analysis of data

This is done by the analyzer engine and applied to the input data. The process of doing work in this phase is as follows:

11.1. Receive new data

Receive new data can be generated by any source of information. Perform preprocessing on new data, so that they can be examined with models in the analyzer engine. In abuse detection, this work is done by converting the information into the desired format, and in anomaly detection, this will be done by modifying the behavioral characteristics and signs of the users and the system. An analysis operation is performed on pre-processed data. This is done by comparing the signs and indications stored previously in the analyzer engine.

Return and modify

In this phase, which runs parallel to the previous phase, corrective action is taken on the analyzer engine. In the mode of abuse detection, the abuse is done by updating the patterns and signs of the attacks, and in anomaly detection, the features made of users' behavior are updated. Due to the fact that intrusion detection methods are divided into two general categories of abuse detection and anomaly detection, the error rate of each one is determined by the artificial neural network method.

12. Artificial Neural Networks

In the development of artificial neural networks, the discussion of assigning input data and hidden layers to the desired value in the excel file is of great importance. Accordingly, we consider the expected Intelligence rate of intrusion Detection System is considered as the Target function. Then, using variables or control parameters, we try to manage the output function based on input data (anomaly intrusion detection, abuse intrusion detection, independent variables). Accordingly, the amount of progress and analysis of the input and hidden layers of the input function is determined by the control variables at each stage (for example, for the abuse detection variable specified in Figure 6. Based on the assumptions made at the outset, we use a review of the control variables based on the dependent variable. So first, as a function, Performance and Validation are examined at each step based on the number of hidden layers, and then the amount of correlation coefficient in each step will be obtained based on the control variables. To test the correlation, four functions (Test, Train, Validation, Best) are considered. The Train function is determined by the input data in the excel file[14]. The Test function is created by the program, taking into account the hidden layers. On the other hand, the more we consider the number of hidden layers, the higher the volume of computation and the more time to calculate. On the other hand, the expressed variance and mean will improve and the standard deviation decreases. Initial validation is based on the normalization of input data.

After initial validation and the formation of the initial test function, the value of the Best function is obtained based on the optimum level of the two Train and Test functions. The results from the Train, Test, Best and Validation functions are discussed below. After initial validation and the formation of the initial test function, the value of the Best function is obtained based on the optimum level of the two Train and Test functions. The results from the Train, Test, Best and Validation functions are discussed below.

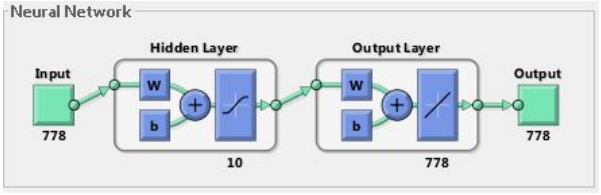

Figure 4: The general structure of the input layers and hidden layers to identify the factors affecting the intrusion detection

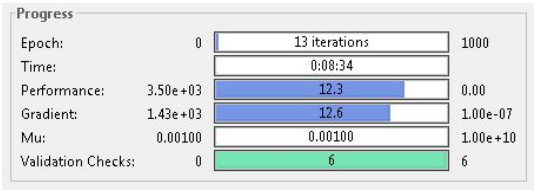

Figure 5: The process of progressing and analyzing the input layer and examining the hidden layer based on intrusion detection variables (intrusion detection)

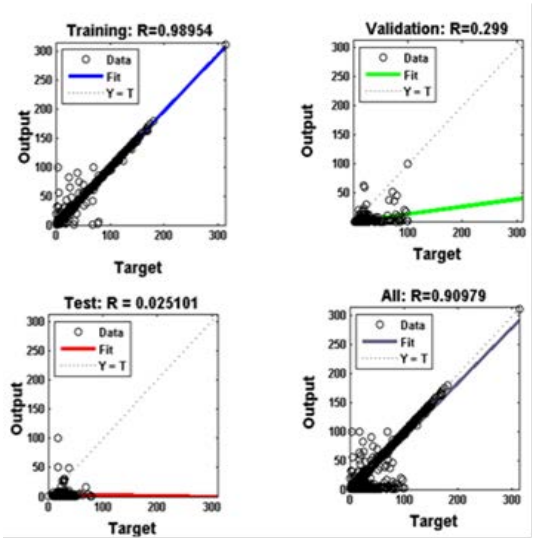

Figure 6: Investigating the Factors affecting Intrusion Detection Using the abuse Detection Method

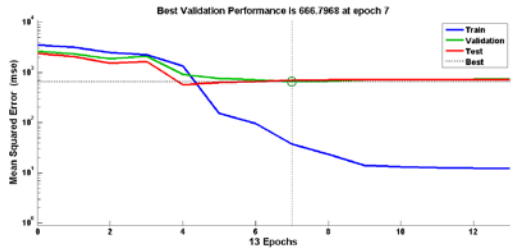

Figure 7: Getting the best prediction with respect to the change of use variable

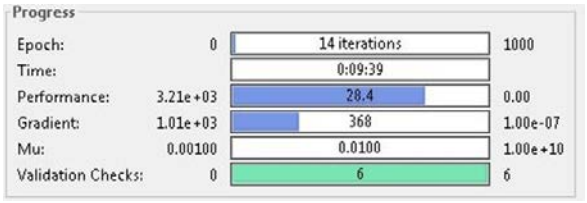

Figure 8: The process of progressing and analyzing the input layer and examining the hidden layer based on intrusion detection variables (anomaly detection)

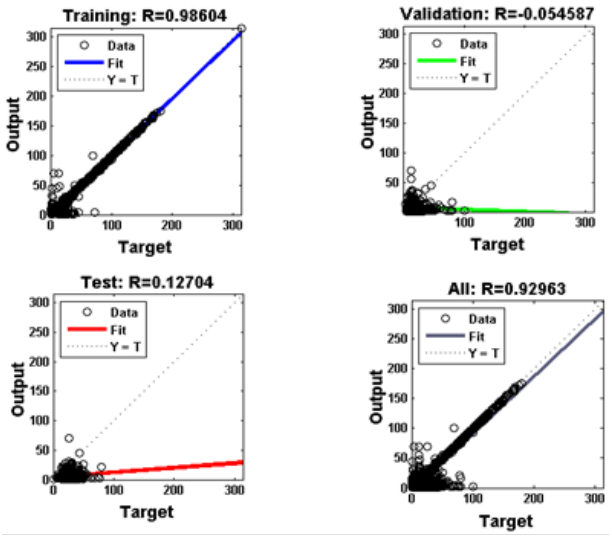

Figure 9: Investigating the Factors affecting intrusion Detection through anomaly Detection

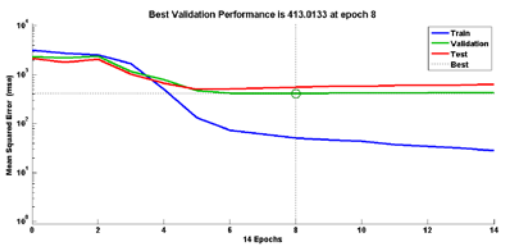

Figure 10: Getting the best prediction with respect to the anomaly variable

13. Conclusion

In general, intrusion detection systems have relatively high weaknesses in detecting new attacks and detecting unusual network behavior. On the other hand, today we need more intelligent software to detect attacks on important networks, including wireless networks, because a smart attacker always chooses smart ways to hide his attacks. The security of a network is created with a good intrusion detection system, but if these systems stop functioning correctly for any reason, difficult will raise in the security system of network. This issue requires an inspection to investigate intrusion detection systems. Inspections can be made in a variety of ways. These methods include centralized or client/server method, local method, and the use of mobile agents[16]. Results were obtained by using different experiments to compare these three states. The local method works more efficiently than the other two methods in terms of system resource consumption, network load, and response time. Further, in the case of failures, the focused approach is similar to the motion-based inspector, which performs better than the centrally-oriented approach. The problem with this group of inspectors is the lack of dynamic changes, which means that if you need to change the working mechanism, it is necessary to change all the inspectors separately, which is a time-consuming operation. According to what said above, the use of such inspectors in small networks is the best way. Attackers may use hiding techniques that many intrusion detection systems do not currently have the ability to detect. It is definitely difficult to detect an attacker, or it is more difficult to detect the type of attack and the attacker's ability to detect the attack, and in general, more sophisticated and smart techniques are needed to detect and deliver the proper function. Therefore, the need for a new approach to intelligent intrusion detection system is imperative. Abuse intrusion detection methods and combined methods (abusive / anomaly) do not have the ability to quickly and accurately detect these attacks due to their weaknesses. Therefore, the use of anomaly Detection methods seems necessary with respect to its ability to detect new attacks. On the other hand, the increasing number of data in the network, and the increase in the amount of data stored in databases, makes it difficult to find complex relationships between data. Therefore, methods should be used to reduce the risk of false alarms in intrusion detection systems, especially the anomaly detection systems, and to analyze the high network traffic that is increasing.

References

[1] S. Chavan, K. Shah, N. Dave, S. Mukherjee, A. Abraham, and S. Sanyal, “Adaptive neuro-fuzzy intrusion detection systems,” itcc, vol. 01, p. 70, 2014.

[2] Anazida Z., Aizaini MM. Mariyam S. “Feature_ Selection Using Rough Set in Intrusion Detection. In” ,Proceeding of the IEEE Region 10 Conference TENCON_ 2006, IEEE, 2006.
[3] Chenfeng Vincent Zhou, Christopher Leckie, Shanika K., "A survey of coordinated attacks and collaborative intrusion detection", Computers Security, Volume: 29, Issue: 1, Elsevier Ltd, Pages: 124-140, 2010.
[4] Feng Jiang, Yuefei Sui, Cungen Cao,"An incremental decision tree algorithm based on rough sets and its application in intrusion detection", Springer, Artif Intell Rev, DOI 10.1007 / s10462-011-9293-z, publish Online: 23 December 2011.
[5] Xinguang TIAN, Xueqi CHENG, Miyi DUAN, Rui LIAO, Hong CHEN, Xiaojuan CHEN, "Network intrusion detection based on system calls and data mining", Springer, Front. Comput. Sci., 4(4): 522–528, DOI 10.1007/s11704-010-0570-9, China 2010.
[6] G. Mohammed N., "Intelligent Data Mining Techniques for Intrusion Detection Models on Network", European Journal of Scientific Research, ISSN 1450-216X Vol.71 No.1, pp. 36-45. 2012.
[7] Taheri Monfared, A. "Introduction to Intrusion Detection Systems." Apa Labs in the field of operating system security, Amir Kabir University of Technology; 2009.
[8] Yufeng Kou, Chang-Tien Lu, S. Sirwong wattana, Yo-Ping Huang,"Survey of Fraud Detection Techniques", In Proceedings of the 2004 IEEE International Conference on Networking , Sensing & Control Taipei, Taiwan, March 21-23, 2004.
[9] M. N. Mohammada, N. Sulaimana, O. A. Muhsinb, "A Novel Intrusion Detection System by using Intelligent Data Mining in Weka Environment", Science Direct, Procedia Computer Science 3 (2011) 1237–1242, 2011.
[10] Ch. Aswani Kumar, K. Bhargavi, and Garima Jalota, "A Note on Implementing Recurrence Quantification Analysis for Network Anomaly Detection", Defence Science Journal, Vol. 62, No. 2, pp. 112-116, DESIDOC, March 2012.
[11] Ali Reza Ghanizadeh, Mohammad Reza Ahadi, “Application of Artificial Neural Networks for Analysis of Flexible Pavements under Static Loading of Standard Axle.” International Journal of Transportation Engineering, Vol.3, No.1, 2015.
[12] S.J.S. Hakim, H. Abdul Razak, Modal parameters based structural damage detection using artificial neural networks – a review, Smart Struct. Syst. 14 (2), pp. 159–189, 2014.
[13] M. Almasifard, "An econometric analysis of financial development's effects on the share of final consumption expenditure in gross domestic product", Eastern Mediterranean University, June 2013.
[14] Khorasani, S. T., & Almasifard, M. (2017). Evolution of Management Theory within 20 Century: A Systemic Overview of Paradigm Shifts in Management. International Review of Management and Marketing, 7(3), 134-137
[15] Foroush Bastani, A., Ahmadi, Z., & Damircheli, D. (2013). A radial basis collocation method for pricing American options under regime-switching jump-diffusion models. Applied Numerical Mathematics, 65, 79-90.
[16] Foroush Bastani, A, Damircheli, D. (2016) An adaptive algorithm for solving stochastic multi-point boundary value problems, Numerical Algorithms 74 (4), 1119-1143.