2010 12th International Conference on Computer Modelling and Simulation

Comparative Analysis of Intrusion Detection Approaches

Iftikhar Ahmad
DCIS, UTP, Bandar Seri Iskandar, 31750, Tronoh, Perak, Malaysia / DSE, CCIS, King Saud University, P.O. Box 51178, Riyadh 11543, Kingdom of Saudi Arabia
wattoohu@gmail.com

Azween B Abdullah
Department of Computer & Information Sciences, Universiti Teknologi, PETRONAS, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia
azweenabdullah@petronas.com.my

Abdullah S Alghamdi
Department of Software Engineering, College of Computer & Information Sciences, King Saud University, P.O. Box 51178, Riyadh 11543, Kingdom of Saudi Arabia
abdksu@gmail.com

Abstract- **Information security is a serious issue especially in present age because a solo attack may cause a big harm in computer and network systems. Several intrusion detection approaches exist to tackle this critical issue but the problem is which one is more suitable in the field of intrusion. Further, these approaches are used in intrusion detection systems. Therefore, in this paper, we evaluated them so that a suitable approach may be advised to intrusion detection systems. This work describes the concepts, tool and methodology being used for evaluation analysis of different intrusion detection approaches using multi-criteria decision making technique. Moreover, conclusion on results is made and direction for future works is presented.**

Keywords- Intrusion Detection System (IDS), Multi-Criteria Decesion Making (MCDM), Intrusion Detection Approaches (IDAs), Artificial Neural Network (ANN), Detection Rate (DR)

I. INTRODUCTION

The active extension of computer networks and particularly internet has raised numerous security issues. During recent years, the number of intrusion has increased extremely. Further, the dependency of private and government corporations are also increasing on their computer and network systems. Therefore, protecting these systems from any intrusion or attack is very significant. Because a single intrusion can cause a big loss or the consistency of the network became unreliable. Therefore, many intrusion detection approaches had been used to ensure the computer and network system secure but the main problem is which approach deals more with the problem of intrusion detection. The most common approaches are statistical, rule based, expert system, pattern recognition and artificial neural network [1, 2].

In this paper, we evaluated and compared these intrusion detection approaches using Analytic Hierarchy Process (AHP). This analysis helped researchers to rank the applied approaches. Moreover, the security implementers may also use such type of analysis in the evaluation of different intrusion detection systems. This paper is divided into sections such as background, related work, intrusion detection approaches (IDAs), implementation, and conclusion. Finally, objective for future work will be described.

II. BACKGROUND

The problem of detecting unauthorized access or use of computer systems on the network is known as intrusion detection. The system that detects and logs inappropriate access is called as intrusion detection system. Denning proposed an intrusion detection model in 1987 which became a milestone in the research in this area. The model which she proposed forms the basic core of most intrusion detection designs in use today [3]. The intrusion detection systems can be classified into three categories as host based, network based and vulnerability assessment based. A host based Intrusion Detection System (IDS) assess information found on a single or multiple host systems, including contents of operating systems, system and application files. While network based Intrusion Detection System (IDS) analyses information captured from network communications by analyzing the stream of packets travelling across the network. Packets are captured through a set of sensors. Vulnerability assessment based Intrusion Detection System (IDS) detects vulnerabilities on internal networks and firewall [2, 4].

Analytic Hierarchy Process (AHP) is a technique for multiple criteria decision-making. It was developed by Saaty in the 1970s and has been broadly studied and polished since then [5]. It supports the decision making process by allowing decision-makers to categorize and calculate the significance of the criteria and alternative solutions of a decision. It helps the decision makers find the one that best suits their requirements rather than assigning a correct decision. Some of the decision situations where AHP is applied are choice, ranking, prioritization, resource allocation, benchmarking and quality management [6, 7].

The intrusion detection systems (IDSs) use diverse type of approaches in their implementations. Therefore, we evaluated them in this research work so that a suitable approach may be proposed for IDSs.

III. RELATED WORK

The AHP has been used in various areas that are numbered in thousands and produced comprehensive results in problems including planning, resource allocation, priority setting, and selection among alternative [8]. In recent times, Berrittella et al. used AHP in deciding how best to reduce

978-0-7695-4016-0/10 $26.00 © 2010 IEEE
DOI 10.1109/UKSIM.2010.112

the impact of global climate change [9]. The Microsoft Corporation used it to quantify the overall quality of software systems [10]. Grandzol and John presented an improved method of the faculty selection process in Higher Education at Bloomsburg University of Pennsylvania [11]. Atthirawong et al. worked on International location decision-making by using AHP [12]. Dey, and Prasanta Kumar used AHP in assessing risk in operating cross-country petroleum pipelines [13]. It is used in deciding how best to manage U.S. watersheds at U.S. Department of Agriculture [12]. Alghamdi presented an approach to evaluate different architecture framework for C4I system using AHP [6]. Saaty and Hsu-Shih Shih worked in the field of decision making by making hierarchy network structure. They stated that creating a structure is the first step in organizing, representing and solving a problem. Actually, a structure is a mode of a problem. It helps us to visualize and understand the relevant elements within it that we know from the real world and then use our understanding to solve the problem represented in the structure with better confidence [15].

Therefore a suspicious consideration is required to build an AHP hierarchy network for evaluating intrusion detection approaches. The Analytic Hierarchy Process is a method of measurement for formulating and analyzing decisions. AHP is a decision support tool which can be used to solve complex decision problems considering tangible and intangible aspects. Therefore, it supports decision makers to make decisions involving their experience, knowledge and intuition [6].

IV. INTRUSION DETECTION APPROACHES (IDAs)

There are many approaches used in intrusion detection systems but we consider five approaches for analysis purpose such as statistical approach, rule based approach, expert system approach, pattern recognition approach and artificial neural network approach.

A brief review of these famous approaches is described below that are landmarks in the development of intrusion detection systems.

A. Statistical approach

This approach involves statistical comparison of specific events based on a predetermined set of criteria. The data was collected from the system and the network. This collected data was tested for attack analysis by statistical models. The models which have been most frequently used include the Operational Model, Average and Standard Deviation Model, the Multivaried Model, the Markovian Model, and the Time Series Model [16, 17]. This was much laborious and time consuming work.

B. Rule based approach

This approach relies on sets of predefined rules which are provided by an administrator, automatically created by the system, or both. Each rule is mapped to a specific operation in the system. The rules serve as operational preconditions which are continuously checked in the audit record by the intrusion detection mechanism. If the required conditions of a rule are satisfied by user activity the specified operation is executed [17, 18]. This approach was unable to detect novel intrusion. A frequent update of rules is required in this approach that is time consuming. Moreover, this approach was unable to detect new attacks.

C. Expert System approach

This approach consists of a set of rules, which encode the knowledge of a human "expert". Unfortunately, Expert Systems require frequent updates by a System Administrator to remain up to date [17]. The lack of maintenance or update is the weakness of this approach.

D. Pattern recognition approach

In this approach, a series of penetration scenarios are coded into the system. This approach is effective in reducing the need to review a large amount of audit data [17, 19]. This is also unable to detect new attacks. Therefore, a frequent updating of penetration scenarios is required.

E. Artificial neural network approach

This approach is a substitute to other approaches. This approach may learn from examples. After training or learning the system is able to detect intrusion. This approach offers the potential to resolve a number of the problems encountered by the other present approaches such as varying nature of attacks. The first advantage in the use of a neural network in the intrusion detection would be the flexibility that the network would provide. A neural network would be able of analyzing the data from the network, even if the data is incomplete or partial. In the same way, the network would have the ability to conduct an analysis with data in a non-linear fashion. Further, because some attacks may be conducted against the network in a coordinated attack by multiple attackers, the capability to process data from a number of sources in a non-linear fashion is particularly important. The problem of regularly updating of traditional intrusion detection systems is also reduced by ANN. It has generalization property and hence able to detect unknown and even variation of known attacks. Another reason to employ ANN in intrusion detection is that, ANN can cluster patterns which share similar features, thus the classification problem in intrusion detection can be solved by this approach. The natural speed of neural networks is another advantage [1, 2, 4, 17].

V. IMPLEMENTATION

The methodology and its implementation is divided into ten steps such as selecting a goal, list criteria, list sub-criteria, determine the alternatives, building hierarchy, assignment of priorities, calculation of weights, consistency check, results and final decision. Figure 1 illustrates methodology.

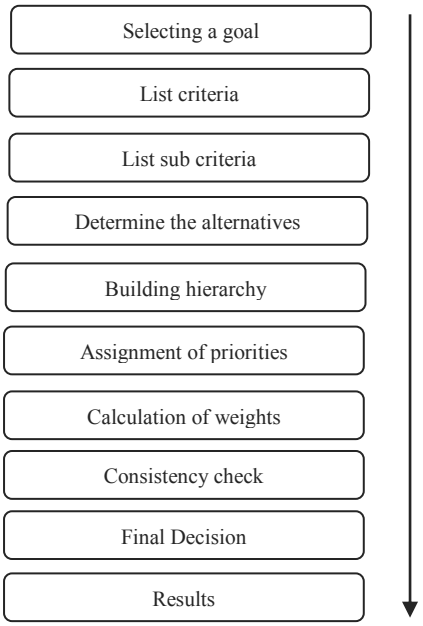

Figure 1. Hierarchy Tree

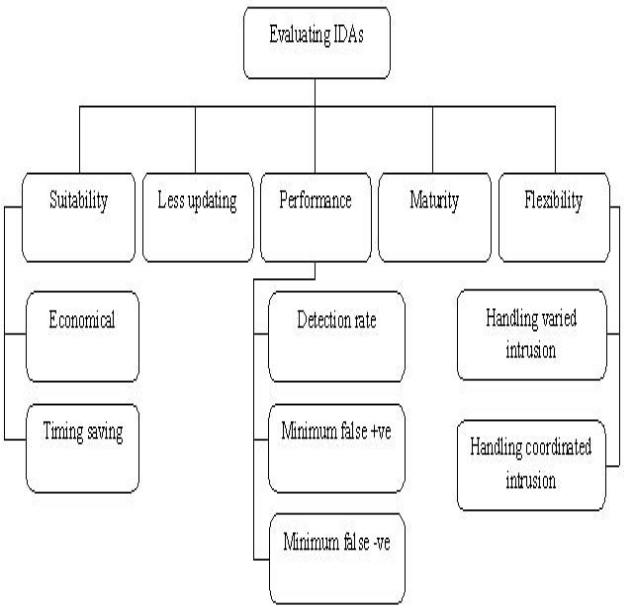

Figure 2. Hierarchy Tree

The details of each step described are;

A. Selecting a goal

First of all, a goal is selected for this experimental work. The goal is evaluating intrusion detection approaches. Five intrusion detection approaches were selected for analysis purpose.

B. List criteria

The next step was the selection of criteria. We build the main criteria that include suitability, less updating, performance, maturity and flexibility.

C. List sub-criteria

The main criteria are further divided into sub-criteria. The criterion "performance" is divided into sub-criteria namely detection rate, minimum false positive and minimum false negative. In the same way, the criterion "suitability" is divided into economical and timing saving. The "flexibility" is further divided into sub-criteria such as handling varied intrusion and handling coordinated intrusion. The selection of criteria and sub-criteria is based on the works as done by many other researchers [1, 2, 17].

D. Determine the alternatives

Five intrusion detection approaches (IDAs) such as statistical approach, rule based approach, expert system approach, pattern recognition approach and artificial neural network approach are decided as alternatives. These approaches are the focus of this research work.

E. Building hierarchy

The hierarchy is built on the bases of criteria, sub-criteria and alternatives. The hierarchy can be visualized as shown in the following diagram figure 2, with the goal (Evaluating IDAs) at the top, the alternatives (ANN, P.R, E.S R.B and statistical) at the bottom (not shown due to complexity), and the criteria (suitability, less updating, performance, maturity and flexibility) and sub-criteria (economical, time saving, detection rate, minimum false positive, minimum false negative, handling varied intrusion, and handling coordinated intrusion) in the middle.

F. Assignment of priorities

The priorities are assigned to criteria, sub-criteria and alternatives. Priorities are numbers associated with the criteria, sub-criteria and alternatives. The assignment of priorities is based on the information obtained from previous works [1, 2, 17]. The scale used for pairwise comparison is shown in Table1.

G. Calculation of weights

The weights of each node/element (criteria, and sub-criteria) are calculated on the bases of assigned priorities as shown in the following tables. The local and global weights of all criteria are shown in Table 2. The sum of all local weights is always equal to 1 and same for the global weights.

The weights of sub-criterion 'suitability' are shown in Table 3. The sum of local weights is equal to 1 and sum of global weights is 0.14 that is the global weight of suitability. The weights of sub-criterion 'performance' are shown in Table 4. The sum of local weights is equal to 1 and sum of global weights is 0.39 that is the global weight of performance.

TABLE I. PRIORITIES ASSIGNMENT

Intensity	Definition
1	Equal importance
2	Weak importance
3	Moderate importance
4	Moderate importance plus
5	Strong importance
6	Strong importance plus
7	Very strong importance
8	Very strong importance plus
9	Extreme importance

TABLE II. CRITERIA WEIGHTS

EVALUATING IDAS {LW=1, GW=1}					
Wgts .	*Suitability*	*Maturity*	*Performance*	*Less updating*	*Flexibility*
LW	0.14	0.08	0.39	0.17	0.22
GW	0.14	0.08	0.39	0.17	0.22

TABLE III. SUB-CRITERIA WEIGHTS

Suitability { LW= 0.14, GW= 0.14}			
Weights	*Economical*	*Time Saving*	*Tot.*
LW	0.25	0.75	1
GW	0.03	0.11	0.14

TABLE IV. SUB-CRITERIA WEIGHTS

Performance { LW= 0.39, GW= 0.39 }				
Weights	*Detection Rate*	*Min. False -*	*Min. False +*	*Tot.*
LW	0.45	0.27	0.28	1
GW	0.18	0.10	0.11	0.39

TABLE V. SUB-CRITERIA WEIGHTS

Flexibility { LW= 0.22, GW= 0.22}			
weights	*Handling Varied Intrusion*	*Handling Coordinated Intrusion*	*Tot.*
LW	.50	.50	1
GW	.11	.11	.22

The weights of sub-criteria 'flexibility' are shown in Table 5. The sum of local weights is equal to 1 and sum of global weights is 0.22 that is the global weight of flexibility.

H. Consistency check

The consistency ratio is calculated based on the weights. If the consistency ratio is <= 10%, the inconsistency is acceptable. If the consistency ratio is > 10%, we need to revise the subjective judgment. In this work the consistency ratio is < 10% so there is no any inconsistency.

I. Results

Results are obtained by the multi criteria software and presented in graphs in the following figures. The bar graph is shown in five different colours such as red represents the criterion suitability, green represents maturity, blue represents performance, yellow represents flexibility, and pink represents less updating. Figure3 shows a ranking among the criteria that are used in the evaluation of intrusion detection approaches. In this case performance is ranked as first, flexibility as second, less updating as third, suitability as fourth and maturity as fifth.

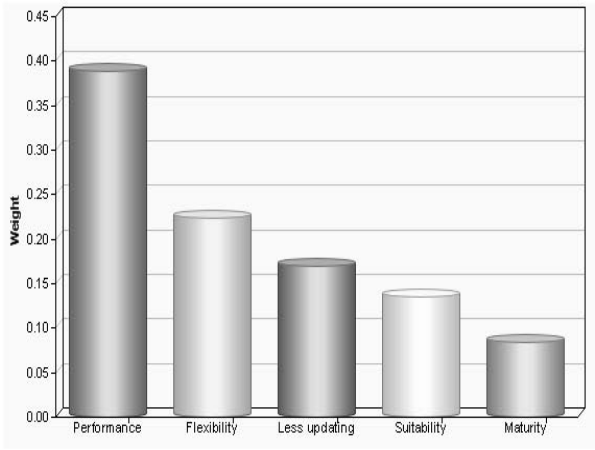

Figure 3. Criteria Ranking

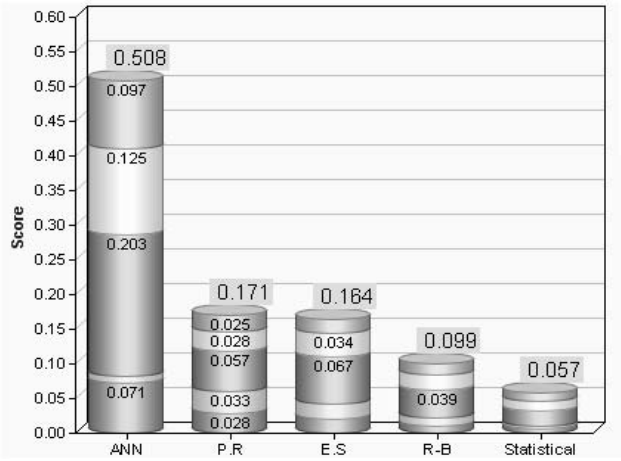

Figure 4. Alternatives Ranking

The ranking of alternatives such as statistical approach, rule based approach, expert system approach, pattern recognition approach and artificial neural network approach is shown in Figure 4. Each alternative consists of five criteria as shown in different colours. For example, the ANN approach is ranked as first suitable approach to tackle present problems to intrusion detection. The red colour in ANN approach in below graph represented a portion of

suitability that is 0.071 of the total criterion suitability. The sum of all alternatives' suitability is equal to total suitability as shown in Figure 2.

Figure 4 shows the ranking of intrusion detection approaches as evaluated in this work. Each approach is evaluated by five different criteria (performance, flexibility, less updating, suitability, maturity) and seven sub-criteria (economical, time saving, detection rate, in. false +ve, min. false-ve, handling varied intrusion, handling coordinated intrusion). The comparative analysis of artificial neural network approach to other approaches is shown in the following figures.

Figure 5 shows a comparison between artificial neural network and rule based approach. The rule based approach is more matured to intrusion detection in Figure 5. However, it is not good in other cases such as time saving, economical, less updating, detection rate, minimum false positive, minimum false negative, handling varied and coordinated intrusion.

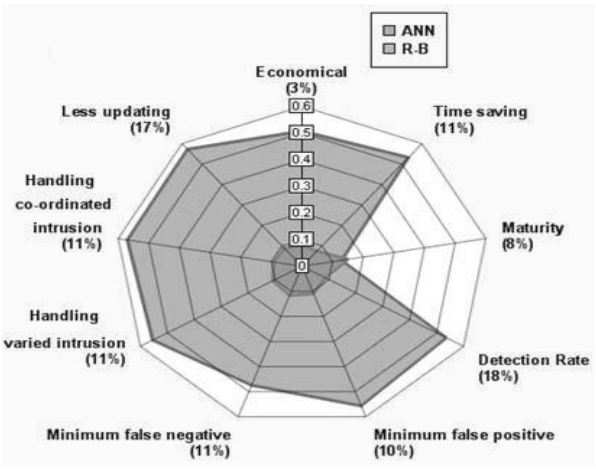

Figure 5. Artificial Neural Network vs. Rule based System

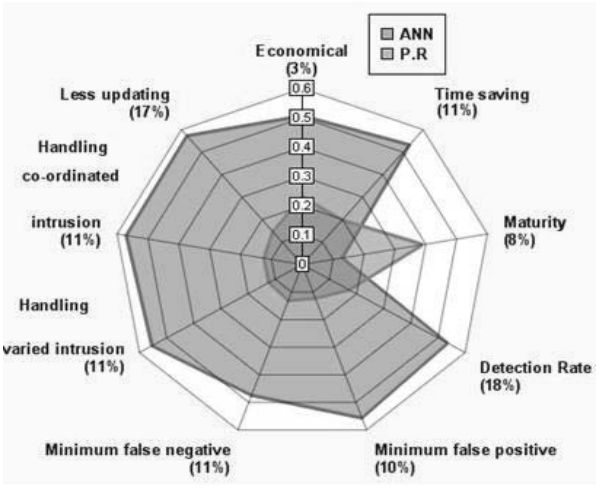

Figure 6. Artificial Neural Network vs. Pattern Recognition

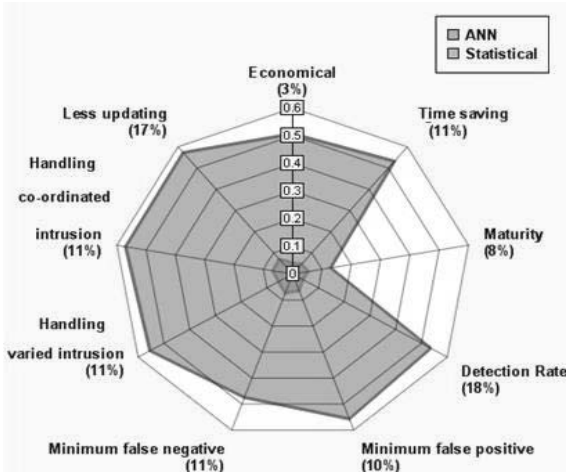

Figure 7. Artificial Neural Network vs. Statistical

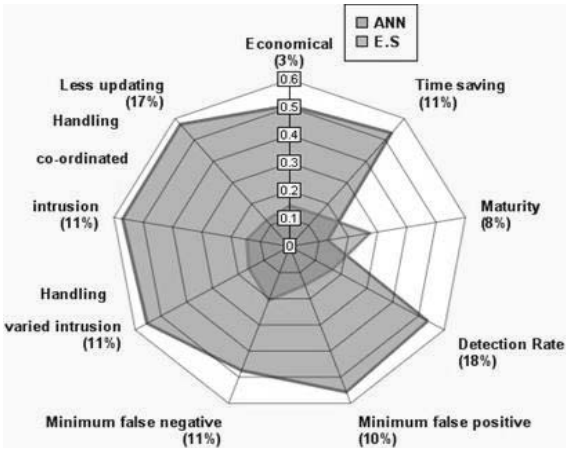

Figure 8. Artificial Neural Network vs. Expert System

Figure 6 shows a comparison between artificial neural network and statistical approach. The statistical approach has many drawbacks for example time consuming, laborious, frequent updating, and unable to detect novel intrusion. Therefore, it is not a good approach to manage presently faced issue of intrusion detection.

Figure 7 shows a comparison between artificial neural network and pattern recognition approach. The pattern recognition approach is much mature in the field of intrusion detection. However, artificial neural network is more suitable in other cases such as time saving, economical, less updating, detection rate, minimum false positive, minimum false negative, handling varied and coordinated intrusion.

Figure 8 shows a comparison between artificial neural network and expert system approach. The expert system approach is more matured in the field of intrusion detection. On the other hand, an artificial neural network approach is more flexible to meet the current issues to intrusion detection. Therefore, the artificial neural network approach is most favourable in case of time saving, economical, less

updating, detection rate, minimum false positive, minimum false negative, handling varied and coordinated intrusion.

J. Final decision

The final decision is based on the results obtained by the multi-criteria software. The results demonstrate that the use of an artificial neural network approach in intrusion detection systems will enhance the security of computer and network systems.

VI. CONCLUSION

Statistical approach, rule based approach, expert system approach, pattern recognition approach and artificial neural network approach are evaluated using Analytic Hierarchy Process. The evaluation is based on two types of criteria for example main criteria and sub-criteria. The main criteria consist of performance, flexibility, less updating, suitability, and maturity. The sub-criteria consist of economical, time saving, detection rate, min. false +ve, min. false-ve, handling varied intrusion, and handling coordinated intrusion. Further, we concluded that artificial neural network approach is more suitable approach among other approaches to tackle present issues to intrusion detection systems such as regular updating, detection rate, false positive, false negative, suitability and flexibility.

VII. FUTURE WORK

A research is needed that will develop an optimized intrusion detection mechanism to identify network activity in a robust way. In this context, we will work on the application of artificial neural networks to intrusion detection that will have a better performance as compared to other approaches.

REFERENCES

[1] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, "Artificial Neural Network Approaches to Intrusion Detection: A Review", in the Book TELECOMMUNICATIONS and INFORMATICS", Included in ISI/SCI Web of Science and Web of Knowledge, Istanbul, Turkey, 2009, pp 200-205.

[2] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, "Application of Artificial Neural Network in Detection of DOS Attacks", In Proceedings of the 2nd international Conference on Security of information and Networks (Famagusta, North Cyprus, October 06 - 10, 2009). SIN '09. ACM, New York, NY, pp 229-234.

[3] Denning, Dorothy. (February, 1987)., "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, Vol. SE-13, No. 2.

[4] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, "Application of Artificial Neural Network in Detection of Probing Attacks", 2009 IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), October 4-6, 2009, Kuala Lumpur, Malaysia.

[5] Saaty, T.L., 2000. Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process. 2nd edition, RWS Publications, Pittsburgh, PA. 478 pp., ISBN 0-9620317-6-3.

[6] Abdullah S. Alghamdi, "Evaluating Defense Architecture Frameworks for C4I System Using Analytic Hierarchy Process" Journal of Computer Science 5(12): 1075-1081, 2009. New York, USA.

[7] Forman, Ernest H. and Saul I. Gass, 2001-07. The analytical hierarchy process-an exposition. Operat. Res., 49: 469-487, doi:10.1287/opre.49.4.469.11231.

[8] Bhushan, Navneet and Kanwal Rai, 2004. Strategic Decision Making: Applying the Analytic Hierarchy Process. Springer-Verlag, London, ISBN: 1-8523375-6-7, p.171.

[9] Berrittella, M., A. Certa, M. Enea and P. Zito, 2007. An Analytic Hierarchy Process for the Evaluation of Transport Policies to Reduce Climate Change Impacts. Fondazione Eni Enrico Mattei (Milano). Available on website on Sept 01, 2009, http://www.feem.it/NR/rdonlyres/A25B9563-2940-423B-A086-6842D51DF29B/2242/1207.pdf.

[10] McCaffrey James, 2005. Test run: The analytic hierarchy process. MSDN Magazine. Available on http://msdn2.microsoft.com/en-us/magazine/cc163785.aspx.

[11] Grandzol, J.R., 2005. Improving the faculty selection process in higher education: A case for the analytic hierarchy process (PDF). IR Applications. http://airweb.org/images/IR%20App6.pdf.

[12] Atthirawong, Walailak and Bart McCarthy, An application of the analytical hierarchy process to international location decision-making. Proceedings of the 7th Annual Cambridge International Manufacturing Symposium: Restructuring Global Manufacturing, University of Cambridge, September 2002, Cambridge, England, ISBN 1-902546-25-3 pp: 1-18.

[13] Dey, P.K., 2003. Analytic hierarchy process analyzes risk of operating cross-country petroleum pipelines in India. Nat. Hazards Rev., 4: 213-221.

[14] De Steiguer, J.E., Jennifer Duberstein and Vicente Lopes, 2003. The analytic hierarchy process as a means for integrated watershed management. Proceedings of the 1st Interagency Conference on Research on the Watersheds, US Department of Agriculture, Agricultural Research Service, Benson, Arizona, October 27-30,. 2003, pp: 736-740.

[15] Saaty, T.L. and H.S. Shih, 2009. Structures in decision making: On the subjective geometry of hierarchies and networks. Eur. J. Operat. Res., Volume 199, Issue 3, 16 December 2009, Pages 867-872, doi:10.1016/j.ejor.2009.01.064.

[16] Huang Kai, Qi Zhengwei, Liu Bo, "Network Anomaly Detection Based on Statistical Approach and Time Series Analysis," waina, pp.205-211, 2009 IEEE International Conference on Advanced Information Networking and Applications Workshops, 2009, Bradford, United Kingdom, May 26-May 29, ISBN: 978-0-7695-3639-2.

[17] Shahbaz Pervez, Iftikhar Ahmad, Adeel Akram, Sami Ullah Swati." A Comparative Analysis of Artificial Neural Network Technologies in Intrusion Detection Systems" WSEAS TRANSACTION ON COMPUTERS, Issue 1, Volume 6, January 2007 (pp.175-180).

[18] Koral Ilgun and Richard A. Kemmerer and Phillip A. Porras, State Transition Analysis: A Rule-Based Intrusion Detection Approach", IEEE Transactions on Software Engineering, 1995, volume 21, pp 181-199.

[19] Davide Ariu, Giorgio Giacinto, Roberto Perdisci , " Sensing attacks in Computers Network with Hidden Markov Models", Machine Learning and Data Mining in Pattern Recognition, MLDM 2007, vol. 4571, Leipzig, Springer-Verlag, pp. 449-463, 2007.