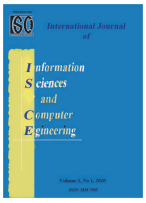
Information Sciences and Computer Engineering, Vol. 1, No. 1, (2010) 60–67

PHARUS

International Journal of
Information Sciences and Computer Engineering

journal homepage: http://www.ijisce.org



Evaluating Intrusion Detection Approaches Using a Multi-criteria Decision Making Technique

Iftikhar Ahmad[a,b,*], Azween Abdullah[b], Abdullah Alghamdi[a]

[a]*Department of Software Engineering, College of Computer & Information Sciences, King Saud University, P.O. Box 51178, Riyadh 11543, Kingdom of Saudi Arabia.*
[b]*Department of Computer & Information Sciences, Universiti Teknologi, PETRONAS, Bandar Seri Iskandar, P.O. Box 31750, Tronoh, Perak, Malaysia.*

***Abstract*– We can witness the growing interest of researchers in the field of intrusion detection because a single attack can easily cause a big harm to the computer or network system. A number of intrusion detection approaches are available to tackle this issue but it is hard to identity that which approach is most suitable. Therefore, we have addressed this issue in this paper that which approach should be adopted in intrusion detection systems. The current paper explains the concepts, tools and methodologies being used to evaluate different intrusion detection approaches by a multi-criteria decision making technique such as Analytical Hierarchy Process (AHP). The present study indicates that artificial neural network approach is most suitable to tackle the current issues of intrusion detection systems such as regular updating, detection rate, false positive, false negative, suitability and adaptability.**

Keyword: Intrusion Detection System (IDS), Multi-Criteria Decesion Making (MCDM), Anlytic Hierarchy Process (AHP), Intrusion Detection Approaches (IDAs), Artificial Neural Network (ANN), Criteria, Hierarchy,Alternative

1. Introduction

Presently, there is an increased need for secure operation in computer systems and networks because computer systems of private and government corporations are relying heavily on networking and internet. Therefore, potential for misuse of these systems increases as accessibility increases. Further, the complexity of modern systems makes detection of malicious activity difficult. Intrusion detection systems are increasingly a key part of systems defense. Various approaches to intrusion detection are currently being used, but they are relatively ineffective. The intrusion detection systems (IDSs) use diverse type of approaches such as statistical, rule based, expert system, pattern recognition, graph-based, hybrid and artificial neural network in their implementations[1, 2]. Therefore, we evaluated and compared them in this paper using multicriteria decision making technique such as Analytic Hierarchy Process (AHP) so that a suitable approach may be proposed for IDSs. This work 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 related work, intrusion detection approaches (IDAs), methodology and implementation, and conclusion.

*Corresponding author:
Email addresses: wattoohu@gmail.com, Ph: +96 6500755849

2. Related work

The process of monitoring the events occurring in a computer system or network and analyzing them for sign of intrusions is known as intrusion detection system (IDS). Denning [1987] proposed an intrusion detection model which became a milestone in the research in this area. The model which she proposed forms the basic core of the majority 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 method for multiple criteria decision-making. It was developed by Saaty [1970s] and has been mainly refined since then [5]. It supports the decision making process by allowing decision-makers to categorize and analyze the significance of the criteria and alternative solutions of a decision. It helps the decision makers to 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]. 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 [7]. In recent times, Berrittella et al. used AHP in deciding how best to reduce the impact of global climate change [8]. The Microsoft Corporation used it to quantify the overall quality of software systems [9]. Grandzol and John presented an improved method of the faculty selection process in Higher Education at Bloomsburg University of Pennsylvania [10]. Atthirawong et al. worked on International location decision-making by using AHP [11]. Dey, and Prasanta Kumar used AHP in assessing risk in operat-

ing cross-country petroleum pipelines [12]. It is used in deciding how best to manage U.S. watersheds at U.S. Department of Agriculture [11]. 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 [13]. 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].

3. Intrusion Detection Approaches (IDAs)

Various approaches have been used in intrusion detection systems but we consider seven approaches for analysis purpose such as statistical approach, rule based approach, expert system approach, pattern recognition approach, graph-based approach, hybrid approach and artificial neural network approach. A brief review of these is described that are landmarks in the development of intrusion detection systems.

3.1. 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 frequently used are Operational Model, Average and Standard Deviation Model, the Multivaried Model, the Markovian Model, and the Time Series Model [14, 15]. The analysis of threats was much laborious and time consuming because first data are collected and then different models are applied.

3.2. 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 [15, 16]. A frequent update of rules is required in this approach that is time consuming. Moreover, this approach was unable to detect new attacks.

3.3. 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 [15]. The lack of maintenance or update is the weakness of this approach. Further, the accurate knowledge acquisition and its encoding is also a complex phenomenon.

3.4. 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 [15, 17]. This is also unable to detect new attacks. Therefore, a frequent updating of penetration scenarios is required. Further, the creating of accurate penetration scenarios and their coding into the system is a serious and complex issue.

3.5. Graph-based approach

In this approach, the data is collected about an activity on computer and network traffic and this information is given to activity graphs that reveal the fundamental structure of network activity. By analyzing the characteristics of the activity graphs, different reports are generated. This analysis is generally done through searching the graphs built for known bad patterns. A policy language to express acceptable and unacceptable behavior on the network is included with this approach so that an administrator can define policies in their departments. This approach has a drawback that an administrator continuously monitors the activities on the screen. Further, it faces other issues such frequent updating, false positive and false negative [18].

3.6. Hybrid approach

This approach is a combination of above two approaches such a graph based approach and statistical approach or any other. In this approach, administrators continuously watch on the screen and observe anomalies behavior. Once anomaly occurred then it is analyzed by different statistical models that are time consuming. Therefore, an accurate and timely detection of intrusion is very necessary [19].

3.7. 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, 15].

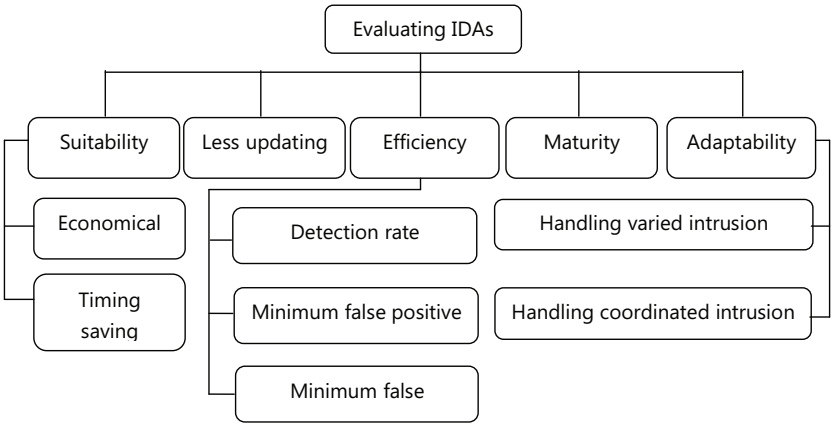


Fig. 1. Hierarchy Tree.

Table 1. Criteria and Sub-Criteria Weights.

Evaluating IDAs LW=1, GW=1										
Suitability {LW = 0.14, GW = 0.14}			Maturity {LW = 0.08, GW = 0.08}	Efficiency {LW = 0.39, GW = 0.39}				Less updating {LW = 0.17, GW = 0.17}	Adaptability LW = 0.22, GW = 0.22		
Economical	Time saving	Tot.		Detection rate	Min. FP	Min. FN	Tot.		Handling varied intrusion	Handling coordinated intrusion	Tot.
0.25	0.75	1		0.45	0.27	0.28	1		0.50	0.50	1
0.03	0.11	0.14		0.18	0.10	0.11	0.39		0.11	0.11	0.22

Note: LW: Locat Weight, GW: Global Weight, FP: False Positove, FN: False Negative

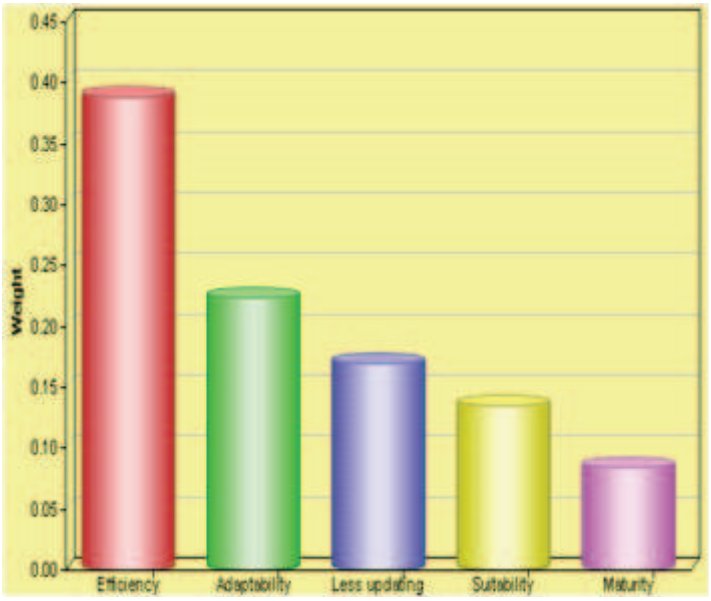


Fig. 2. Multiple criteria analysis.

4. Methodology and Implementation

The methodology consists of 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. Further, this work is implemented using a multi-criteria decision making software e.g. AHP project. First of all, a goal is selected for this experimental work. The

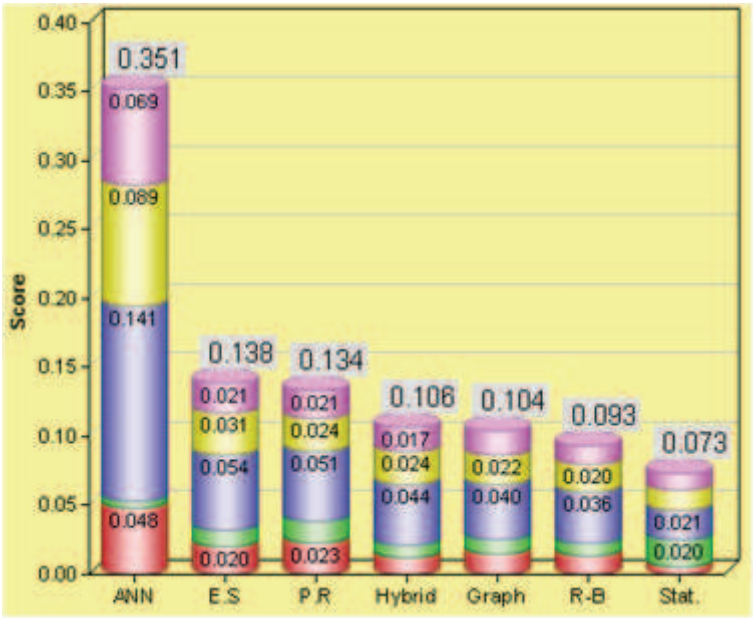


Fig. 3. IDAs Comparative Analysis.

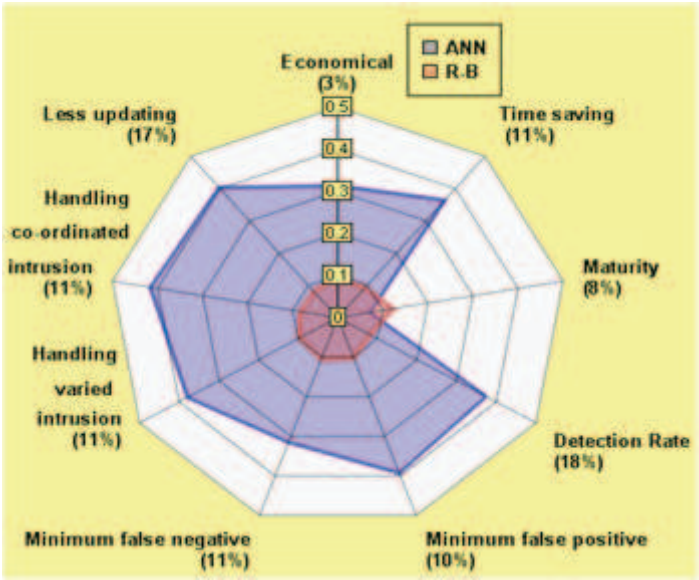


Fig. 4. Artificial Neural Network vs. Rule-based.

goal is evaluating intrusion detection approaches. Seven intrusion detection approaches are selected for analysis. The next step is the selection of criteria. We build main criteria that include 'suitability', 'less updating', 'efficiency', 'maturity' and 'adaptability'. The main criteria are further divided into sub-criteria. The criterion 'efficiency' 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 'adaptability' 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, 15]. Seven intrusion detection approaches (IDAs) such as statistical approach, rule based approach, expert system approach, pattern recognition approach, graph-based approach, hybrid approach and artificial neural network approach are decided as alternatives. These approaches are the focus of this work. The hierarchy is built on the bases of criteria, sub-criteria and alternatives. The hierarchy can be visualized as shown in Figure 1, with the goal (Evaluating IDAs) at the top, the alternatives (ANN, P.R, E.S R.B, graph-based, hybrid and statistical) at the bottom (not shown due to complexity), and the criteria (suitability, less updating, efficiency, maturity and adaptability) and sub-criteria (economical, time saving, detection rate, minimum false positive, minimum false negative, handling varied intrusion, and handling coordinated intrusion) in the middle. 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, 15]. The scale used for pair-

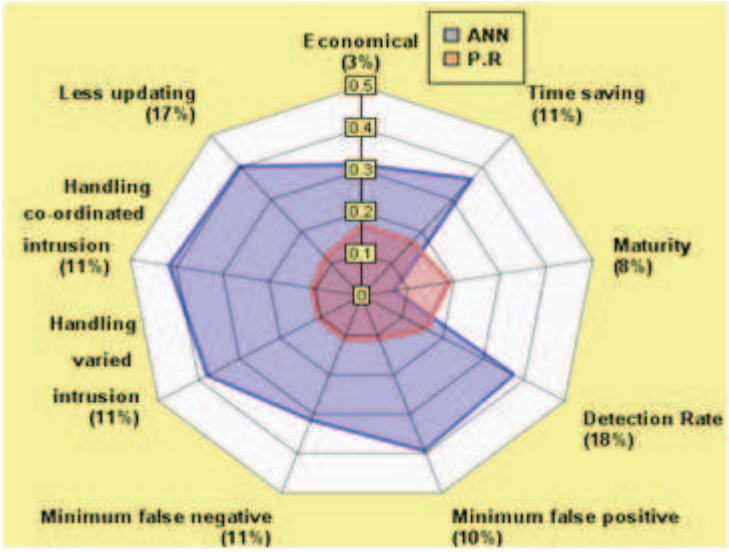


Fig. 5. Artificial Neural Network vs. Pattern Recogination.

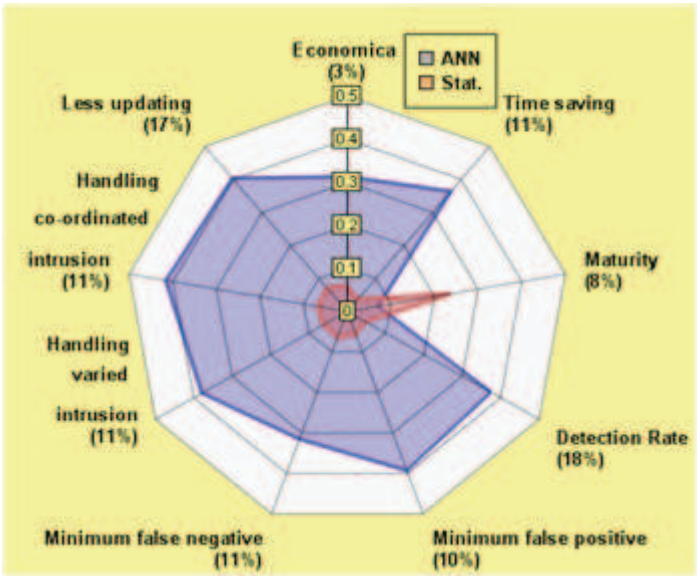


Fig. 6. Artificail Neural Network vs. Statistical.

wise comparison is nine points scale [6]. The weights of each element (criteria, and sub- criteria) are calculated on the bases of assigned priorities as shown in Table1. The local and global weights of all criteria are shown in Table 1. 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 1. 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 'efficiency' are shown in Table 1. The sum of local weights is equal to 1 and sum of global weights is 0.39 that is the global weight of efficiency.

The weights of sub-criteria 'adaptability' are shown in Table 1. The sum of local weights is equal to 1 and sum of global weights is 0.22 that is the global weight of adaptability. The consistency ratio is calculated based on the weights. If the consistency ratio is less than 10 percent, the inconsistency is acceptable. Otherwise, we need to revise the subjective judgment. In this work the consistency ratio is less than 10 percent so there is no any inconsistency. Figure 2 shows a ranking among the criteria that are used in the evaluation of intrusion detection approaches. Results are obtained by the multi criteria software and are presented in graphs. The bar graph in Figure 2 is shown in five different colours. In this case efficiency is ranked as first, adaptability as second, less updating as third, suitability as fourth and maturity as fifth. The ranking of alternatives such as statistical approach, rule based approach, expert system approach, pattern recognition approach, graph-based approach, hybrid approach and artificial neural network approach is shown in Figure 3. Each alternative consists of five criteria as shown in different colours. The ANN approach is ranked as first suitable approach to tackle present problems to intrusion detection. The red colour in ANN approach in Figure 3 indicates a portion of suitability that is 0.048 of the total criterion suitability. The sum of all alternatives. suitability is equal to total suitability as shown in Figure 2.

Figure 3 shows the ranking of intrusion detection approaches. Each approach is evaluated by five different criteria (efficiency,

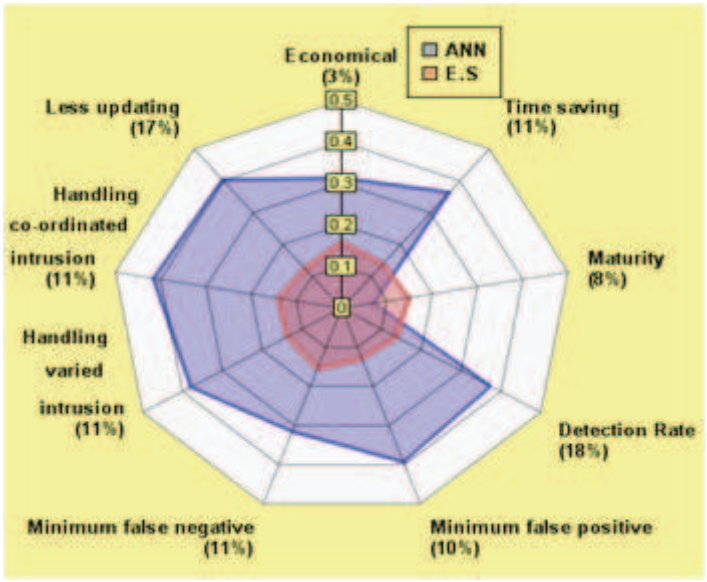


Fig. 7. Artificial Neural Network vs. Expert System.

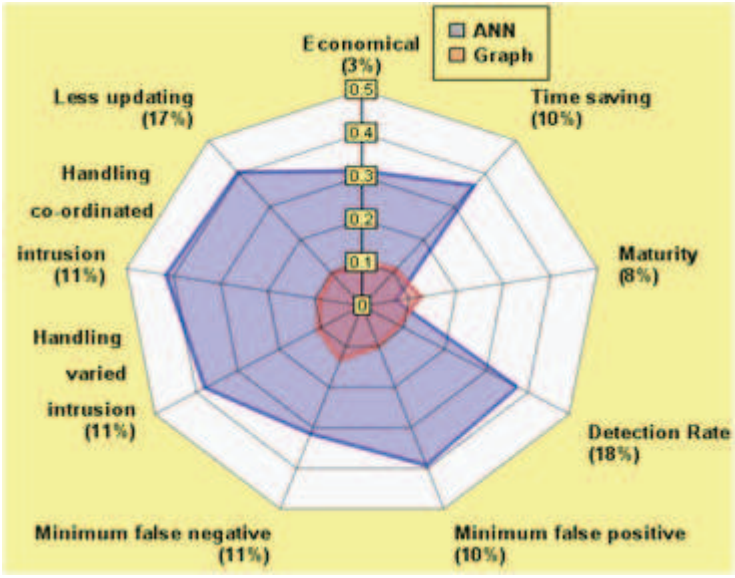


Fig. 8. Artificial Neural Network vs. Graph-based.

adaptability, less updating, suitability, and maturity) and seven sub-criteria (economical, time saving, detection rate, min. false positive, min. false negative, handling varied intrusion, and handling coordinated intrusion). The comparative analysis of artificial neural network approach to other approaches is shown in figures 4– 9. Figure 4 shows a comparison between artificial neural network and rule based approach. The rule based approach is more matured to intrusion detection in Figure 4. 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 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 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 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. Figure 8 shows a comparison between artificial neural network and graph-based approach. Figure 9 shows a comparison between artificial neural network and hybrid approach. In both

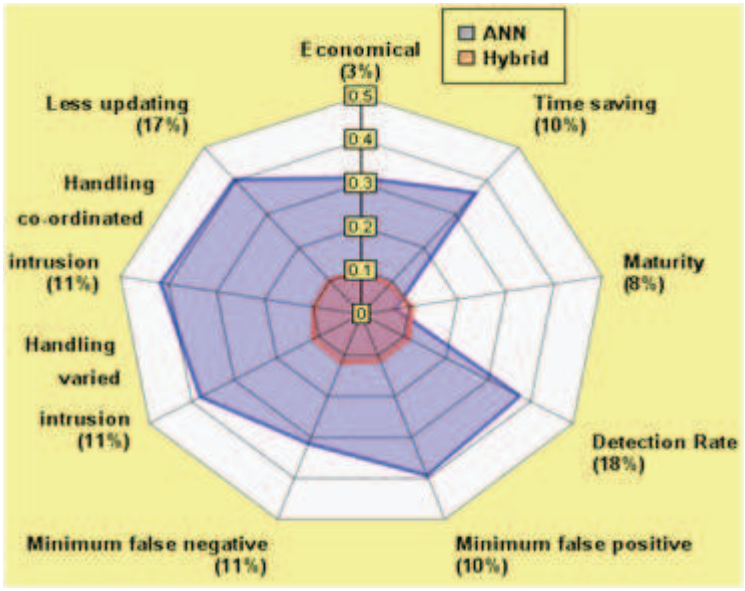


Fig. 9. Artificial Neural Network vs. Hybrid.

cases, artificial neural network is preferable on the basis of defined criteria. 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.

5. Conclusion

The analytical hierarchy process has been used to evaluate different approaches such as statistical approach, rule based approach, expert system approach, pattern recognition approach, graph-based approach, hybrid approach and artificial neural network approach. The evaluation process takes into account two different types of criteria i.e. main criteria and sub-criteria. The strength of main criteria is based on its efficiency, adaptability, less updating, suitability and maturity, while the sub-criteria consists of economical, time saving, detection rate, minimum false positive, minimum false negative and having the capability to handle varied intrusion and also coordinated intrusion. According to our study, we have concluded that among all the approaches, the artificial neural network approach is most suitable to tackle the current issues of intrusions detection systems such as regular updating, detection rate, false positive, false negative, suitability and adaptability.

Acknowledgments

Special thanks to Dr. Muhammad Khurram and Dr. Mohsin Iftikhar for their valuable suggestions .

References

[1] I. Ahmad, A. B. Abdullah, and A. S. Alghamdi, "Artificial neural network approaches to intrusion detection: A review," pp. 200–205, 2009.

[2] I. Ahmad, A. B. Abdullah, and A. S. Alghamdi, "Application of artificial neural network in detection of DOS attacks," *Proceedings of the 2nd international Conference on Security of information and Networks*, pp. 229–234, 2009.

[3] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, vol. 13, no. 2, pp. 222–232, 1987.

[4] I. Ahmad, A. B. Abdullah, and A. S. Alghamdi, "Application of artificial neural network in detection of probing attacks," *IEEE Symposium on Industrial Electronics and Applications*, pp. 557 – 562, 2009.

[5] T. Saaty, *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*. RWS Publications, 2nd ed., 2000.

[6] A. S. Alghamdi, "Evaluating defense architecture frameworks for C4I system using analytic hierarchy process," *Journal of Computer Science*, pp. 1075–1081, 2009.

[7] N. Bhushan and K. Rai, *Strategic Decision Making: Applying the Analytic Hierarchy Process*. Springer-Verlag, 2004.

[8] M. Berrittella, A. Certa, M. Enea, and P. Zito, "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.

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

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

[11] w. Atthirawong and B. 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*, pp. 1–18, 2002.

[12] P. Dey, "Analytic hierarchy process analyzes risk of operating cross-country petroleum pipelines," *Natural Hazards Review*, vol. 4, no. 4, 2003.

[13] T. L. Saaty and H. S. Shih, "Structures in decision making: On the subjective geometry of hierarchies and networks," *European Journal of Operational Research*, vol. 199, no. 3, pp. 867–872, 2009.

[14] H. Kai, Q. Zhengwei, and L. B. Waina, "Network anomaly detection based on statistical approach and time series analysis," pp. 205–211, 2009.

[15] S. Pervez, I. Ahmad, A. Akram, and S. U. Swati, "A comparative analysis of artificial neural network technologies in intrusion detection systems," *WSEAS Transation on Computers*, vol. 6, no. 1, pp. 175–180, 2007.

[16] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State transition analysis: A rule-based intrusion detection approach," *IEEE Transactions on Software Engineering*, vol. 21, no. 3, pp. 181–199, 1995.

[17] D. Ariu, G. Giacinto, and R. Perdisci, "Sensing attacks in computers network with hidden markov models," *Machine Learning and Data Mining in Pattern Recognition*, vol. 4571, pp. 449–463, 2007.

[18] T. Le and C. N. Hadjicostis, "Graphical inference for multiple intrusion detection, information forensics and security," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 370–380, 2008.

[19] S. Peddabachigari, A. Abraham, C. Grosan, and J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems," *Journal of Network and Computer Applications*, vol. 30, no. 1, pp. 114–132, 2007.

Iftikhar Ahmad received the B.Sc. degree in Mathematics and Physics from Islamia University, Bahawalpur, Pakistan, in 1999 and the M.Sc. Computer Science from University of Agriculture, Faisalabad, Pakistan in 2001. He obtained his MS/M.Phil degree in Computer Science from COMSATS Institute of Information Technology, Abbottabad, Pakistan in 2008. Presently he is a Ph.D. candidate at Universiti Teknologi PETRONAS, Malaysia as well as working as research fellow at ASERLab. DSE, CCIS, King Saud University, Saudi Arabia. He has extensive experience of teaching subjects and network management. Moreover, he has different industrial certifications such as MCSE, CCNA, Linux (OS) and CCAI. He has published several papers in highly reputed international conferences and journals. He is member of IEEE, IAENG and IACSIT. His research interests include Computer Networks, Network Security, Intrusion Detection, Neural Networks, Analytic Hierarchy Process, and C4I systems.

Azween Abdullah obtained his bachelor degree in Computer Science in 1985, Master in Software Engineering in 1999 and his Ph.D. in computer science in 2003. His work experiences includes twenty years in institutions of higher learning in both the management and academic capacities, and fifteen years in commercial companies as Software Developer and Engineer, Systems Analyst and IT/MIS and educational consultancy and training. He has spent more than a decade with leading technology firms and universities as a process analyst, senior systems analyst, project manager, and lecturer. He have participated in and managed several software development projects. These have included the development of management information systems, software process improvement initiatives design and implementation, and several business application projects.

His area of research specialization includes computational biology, system survivability and security, autonomic computing and self-healing and regenerating systems, formal specifications and network modeling. His contributions include publishing several journal and refereed conference papers and in the development of programs to enhance minority involvement in bridging the ICT digital gap. Currently he is working on two projects funded by the Ministry of Science Technology and Innovation.

Dr. Abdullah Alghamdi is a full time associate professor, SWE Department, College of Computer and Information Sciences, KSU. He holds a Ph.D. in the field of Software Engineering from the department of computer science, Sheffield University, UK, 1997. He obtained his M.Sc. in the field of software development technologies from the UK in 1993. In the academic year 2004/5 he worked as a visiting professor at School of IT and Engineering, University of Ottawa, Ottawa, Canada, where he conducted intensified research in Web Engineering as part of his Post-Doc program. He recently published a number of papers in the field of Web engineering methodologies and tools. Dr. Abdullah worked as a part-time consultant with a number of governmental and private organizations in the field of IT strategic planning and headed a number of IT committees inside and outside KSU. Currently he is chairing the Software Engineering Department at KSU and part time consultant at Ministry of Defense and Aviation.