International Journal of the Physical Sciences Vol. 5(12), pp. 1830-1839, 4 October, 2010
Available online at http://www.academicjournals.org/IJPS
ISSN 1992 - 1950 ©2010 Academic Journals

Full Length Research Paper

Towards the selection of best neural network system for intrusion detection

Iftikhar Ahmad[1,2]*, Azween Abdullah[1] and Abdullah Alghamdi[2]

[1]Department of Computer and Information Sciences, Universiti Teknologi Petronas, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia.
[2]Department of Software Engineering, College of Computer and information Sciences, P. O. Box 51178, Riyadh 11543, King Saud University, Saudi Arabia.

Accepted 13 July, 2010

Currently, network security is a critical issue because a single attack can inflict catastrophic damages to computers and network systems. Various intrusion detection approaches are available to adhere to this severe issue, but the dilemma is, which one is more suitable. Being motivated by this situation, in this paper, we evaluate and compare different neural networks (NNs). The current work presents an evaluation of different neural networks such as Self-organizing map (SOM), Adaptive Resonance Theory (ART), Online Backpropagation (OBPROP), Resilient Backpropagation (RPROP) and Support Vector Machine (SVM) towards intrusion detection mechanisms using Multi-criteria Decision Making (MCDM) technique. The results indicate that in terms of performance, supervised NNs are better, while unsupervised NNs are better regarding training overhead and aptitude towards handling varied and coordinated intrusion. Consequently, the combined, that is, hybrid approach of NNs is the optimal solution in the area of intrusion detection. The outcome of this work may help and guide the security implementers in two possible ways, either by using the results directly obtained in this paper or by extracting the results using other similar mechanism, but on different intrusion detection systems or approaches.

Key words: Neural networks (NN), multi-criteria decision making (MCDM), intrusion detection system (IDS), analytic hierarchy process (AHP).

INTRODUCTION

The dynamic expansion of computer networks in general 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 inevitable. Because a sole intrusion can cause an immense loss or the reliability of the network can prove defective or susceptible to threats.

The dilemma of detecting unauthorized access or use of computer systems on the network is known as intrusion detection. The system that detects and logs improper access is called as intrusion detection system.

*Corresponding author. E-mail: wattoohu@gmail.com.

Denning (1987) proposed an intrusion detection model, which became a milestone in this research area. The proposed model forms the basic core of most intrusion detection designs in use today.

The intrusion detection systems can be classified into three categories as host based, network based and vulnerability assessment based. A host based IDS assess information is found on a single or multiple host systems, including contents of operating systems, system and application files. While network based IDS analyses information is captured from network communications, analyzing the stream of packets travelling across the network. Packets are captured through a set of sensors. Vulnerability assessment based IDS detects vulnerabilities on internal networks and firewall (Ahmad et al., 2009a).

One of the most important techniques for multiple criteria decision-making was developed by Saaty in the

1970s. It has been mostly considered and practiced since then (Saaty, 2000a). It supports the decision making process by allowing decision-makers to classify and analyze the impact of criteria and alternative solutions of a decision. It assists the decision makers in finding the one that best suits their requirements rather than assigning a correct decision. Some of the decision situations where MCDM is applied are choice, ranking, prioritization, resource allocation, benchmarking and quality management (Forman and Gass (2001).

Therefore, many intrusion detection techniques had been used to ensure the security of computer and network system, but the main problem was, which technique dealt effectively with the problem of intrusion detection. The most common artificial neural networks are adaptive resonance theory (ART), resilient backpropagation (RPROP), online backpropagation (ORPROP), self organizing map (SOM) and support vector machine (SVM) (Ahmad et al., 2009a, 2009b).

The neural network intrusion detection mechanisms (NNIDMs) use different types of techniques in their implementations. Therefore, we are evaluating them, so that a suitable NN may be advised for intrusion detection.

In this paper, we evaluated and compared these artificial neural networks using multi-criteria decision making (MCDM) technique. This analysis helped researchers to rank the applied techniques. Moreover, the security implementation units can also refer such type of analysis in the evaluation of different intrusion detection systems.

Related work

The MCDM 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 (Bhushan and Kanwal, 2004). In recent times, Berrittella et al. (2007) used analytic hierarchy process (AHP) in deciding how best to reduce the impact of global climate change. The microsoft corporation used it to quantify the overall quality of software systems (James, 2005). Grandzol (2005) presented an improved method of the faculty selection process in Higher Education at Bloomsburg University of Pennsylvania. Atthirawong and McCarthy (2002) worked on International location decision-making by using AHP. Dey (2003) used AHP in assessing risk in operating cross-country petroleum pipelines. It is used in deciding how best to manage U.S. watersheds at U.S. Department of Agriculture, Alghamdi (2009) presented an approach to evaluate different architecture framework for C4I system using AHP. Saaty and Shih (2009b) 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. Steiguer et al. (2003) described that 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. Therefore, a suspicious consideration is required to build AHP hierarchy network for evaluating intrusion detection approaches. The analytic hierarchy process is a method of measurement in 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 (Alghamdi, 2009; Kunio et al., 2009; Chien, 2010).

The neural network intrusion detection is a replacement to other traditional 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 issues experienced by the existing approaches, such as varying nature of attacks. The first advantage in the use of a neural network in the intrusion detection is the flexibility that the network provides. A neural network is capable of analyzing the data from the network, even if the data are incomplete or partial. In the same way, the network has the ability to conduct an analysis with data in a non-linear fashion. Further, as some attacks may be induced against the network coordinated by multiple attackers, the capability to process data from a number of sources in a non-linear fashion is of monumental importance. The problem of regularly updating the traditional intrusion detection systems is also reduced by ANN (Ahmad et al., 2009c). It has the generalization property and hence is able to detect the variations of unknown and known attacks as well. 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 (Ahmad et al., 2010).

The earlier work of Ahmad et al. (2009c) emphasized that data can be obtained by three ways; by using real traffic, using sanitized traffic and also, using simulated traffic, but IDS are tested mainly on a standard dataset KddCup99 MIT lab. USA. Different researcher used different neural network architecture like ART, SOM, SVM, OBPROP, and RPROP to implement their proposed systems in the field of intrusion detection. Mostly, parameters for testing results are false positive, false negative, detection rate and ROC. They used MATLAB, PlaNet, OPNET, JOONE, URANO, NeuralWorks simulators and some are developed in a personalized way. There is no doubt that NN minimize various flaws in traditional IDSs like time consuming statistical analysis, regular updating, non adaptive, efficiency, accuracy and flexibility. Thus, it also suffers

many problems in the research of intrusion detection. There are two types of training/learning supervised and unsupervised that are used in NIDS. The first involves training overheads (time consuming, regular update and unable to detect novel attack), while the second one is not much more optimized in performance (false positive, false negative and detection rate). Application of NN in intrusion detection is an ongoing area and is limited to academic research till now. Therefore, an optimized NN architecture is required to the problem of intrusion detection.

NEURAL NETWORKS

Several neural networks have been used in intrusion detection, but we considered five for analysis: Self-organizing map (SOM), adaptive resonance theory (ART), online backpropagation (OBPROP), resilient backpropagation (RPROP) and support vector machine (SVM). The reason for selecting these networks was based on their wider usability in the area of intrusion detection. A short review of these renowned NNs is described as landmarks in the development of intrusion detection systems.

Self-organizing map (SOM)

The SOM was developed by Prof. Teuvo Kohonen in the early 1980s. The self-organizing map (SOM) neural network is used to recognize anomalies in network data stream (Min and Wang, 2009). Unlike other approaches, which use self organizing maps to process the entire state of a network or computer system to detect anomalies, proposed system breaks down the system by using collection of more specialized maps. A monitor stack was constructed and each neural network become kind of specialist in recognizing normal behaviour of a protocol and raise an alarm when a deviation from normal profile occurs. This approach is good in case of novel detection, but it has less performance in case of detection rate. This approach gives many false alarms, if it is not properly designed and trained.

Adaptive resonance theory (ART)

Adaptive resonance theory (ART) is developed by Stephen G and Gail C. The ART is a neural network that uses unsupervised learning. The ART net has many flavours such as ART1, ART2, ART2A, ART3, Fuzzy ART, ARTMAP and Fuzzy ARTMAP. This is used by many researches in the field of intrusion detection. ART nets can efficiently classify network traffic into normal and intrusive (Morteza et al., 2006). Further, it may be used as a hybrid of misuse and anomaly detection approaches. Therefore, it is capable of detecting known attack types as well as new attack types as anomalies.

Online backpropagation (OBPROP)

The backpropagation is a supervised neural network and is mostly used by many researchers in the field of intrusion detection. A neural network learns to resolve a problem simply by modifying its internal connections (biases and weights) by back-propagating the difference between the current output of the neural network and the desired response. In order to obtain that, each bias/weight of the network's components (both layers and synapses) is adjusted according to some specific algorithm. Online backpropagation (OBPROP) adjusts the Layers' biases and the Synapses' weights according to the gradient calculated and back-propagated by the backward-transportation mechanism. It is called 'On-Line' because it adjusts the biases and weights after each input pattern is read and elaborated, so each new pattern will be elaborated using the new weights/biases calculated during the previous cycles (Yatim et al., 2006). In on-line learning, each propagation is followed immediately by a weight update. It requires more updates. This net shows optimum performance on known intrusion, but is unable to detect unknown attacks.

Resilient backpropagation (RPROP)

RPROP is developed by (Riedmiller and Braun, 1993). Resilient Backpropagation (RPROP) is an improved adaptation of the batch backprop algorithm, and for numerous problems it converges very quickly. It uses only the sign of the backpropagated gradient to change the biases/weights of the network, instead of the magnitude of the gradient itself. This is because, when a Sigmoid transfer function is used, the gradient can have a very small magnitude, causing small changes in the weights and biases, even though the weights and biases are far from their optimal values. This modified algorithm is a batch training algorithm and uses only the batch size property. The value of the learning rate and the momentum properties does not affect the calculus of the RPROP algorithm (Dutta et al., 2004). This net shows optimum performance on known intrusion, but is unable to detect unknown attacks.

Support vector machine (SVM)

Support vector machines (SVM) are a group of supervised learning methods that can be applied to classification or regression. Support vector machines represent an extension to nonlinear models of the generalized portrait algorithm. The SVM algorithm is

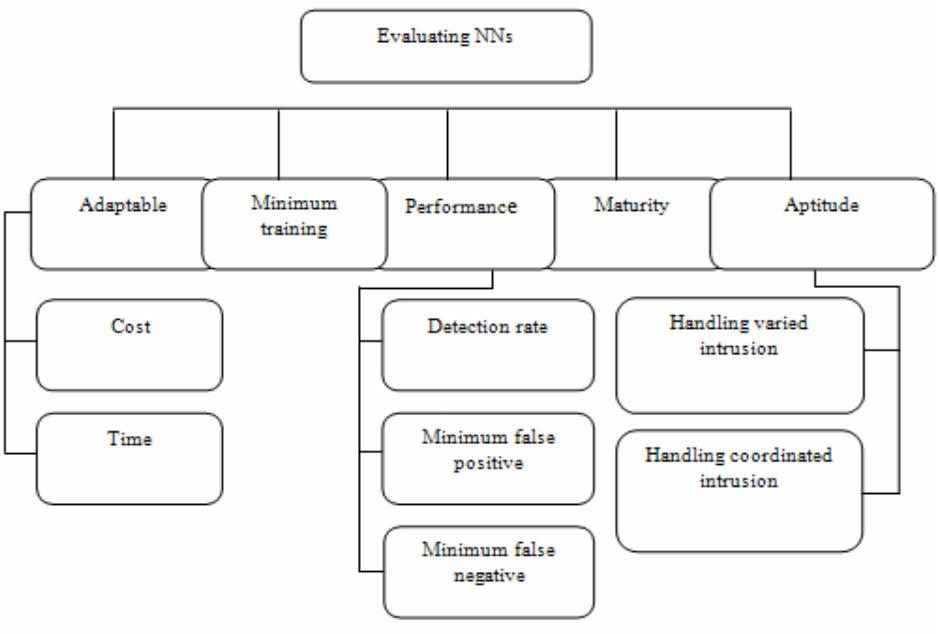

Figure 1. Multi-criteria tree.

based on the statistical learning theory. It is strictly used for small to medium sized classification problems (Latifur et al., 2007). The SVM is especially effective in separating sets of data that share complex boundaries. This net shows optimum performance on known intrusion, but lapses to detect unknown attacks. SVM constructs a hyperplane or set of hyperplanes in a high or infinite dimensional space, which can be used for classification, regression or other tasks. Intuitively, a good separation is achieved by the hyperplane that has the largest distance to the nearest training data points of any class, since in general, the larger the margin, the lower the generalization error of the classifier.

METHODOLOGY AND IMPLEMENTATION

The methodology introduced in this work consist of ten steps such as selecting a goal, list criteria, list sub criteria, determining the alternatives, building hierarchy, assignment of priorities, calculation of weights, consistency check, comparative analysis, results and discussions. The detail of each step is described.

Selecting a goal

Firstly, a goal is selected of our experimental work. The goal is, evaluating NNs for intrusion detection. Five NNs were selected for analysis purpose.

List criteria

The next step is the selection of criteria. Here, the main criteria are built, which includes adaptable, minimum training, performance, maturity and aptitude. The criterion “adaptable” refers to the ability of NN that is affordable in the case of implementation and complexity that can be determined on cost and time parameters. The criterion “minimum training” refers to the learning ability of NN. The criterion “performance” describes the classification capability of NN in case of network packet analysis. The “maturity” refers to the effectiveness of NN in the area of intrusion detection. The “aptitude” refers to the ability of NN to handle varied and coordinated intrusion.

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 “adaptable” is divided into cost and time. The “aptitude” 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 done by many other researchers (Yatim et al., 2006; Ahmad et al., 2010; Morteza et al., 2006).

Determine the alternatives

Five neural networks such as ART, SOM, RPROP, OBPROP, and SVM are decided as alternatives.

Building hierarchy

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 NNs) at the top, the alternatives (ART, SOM, SVM, OBPROP and RPROP) at the bottom (not shown due to complexity), and the criteria (adaptable, minimum training, performance, maturity and aptitude) and sub criteria (cost, time,

Table 1. 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 2. Main criteria weights.

Evaluating NNs {LW = 1, GW = 1}					
Weights	**Adaptable**	**Minimum training**	**Performance**	**Maturity**	**Aptitude**
LW	0.14	0.17	0.39	0.08	0.22
GW	0.14	0.17	0.39	0.08	0.22

Table 3. Performance sub-criteria weights.

Performance { LW = 0.39, GW = 0.39 }				
Weights	**Detection rate**	**Minimum false negative**	**Minimum false positive**	**Total**
LW	0.42	0.29	0.29	1
GW	0.17	0.11	0.11	0.39

Table 4. Adaptable sub-criteria weights.

Adaptable { LW = 0.14, GW = 0.14}			
Weights	**Cost**	**Time**	**Total**
LW	0.25	0.75	1.0
GW	0.04	0.10	0.14

Table 5. Aptitude sub-criteria weights.

Aptitude { LW = 0.22, GW = 0.22}			
Weights	**Handling varied intrusion**	**Handling coordinated intrusion**	**Total**
LW	0.50	0.50	1
GW	0.11	0.11	0.22

detection rate, minimum false positive, minimum false negative, handling varied intrusion, and handling coordinated intrusion) in the middle.

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 (Dutta et al., 2004; Yatim et al., 2006, Ahmad et al., 2009, 2010). The scale used for pair wise comparison is shown in Table 1.

Calculation of weights

The weights of each node/element (criteria, and sub criteria) are calculated on the basis of assigned priorities as shown in Tables 2 to 5. Further, the assignment of priorities is based on the

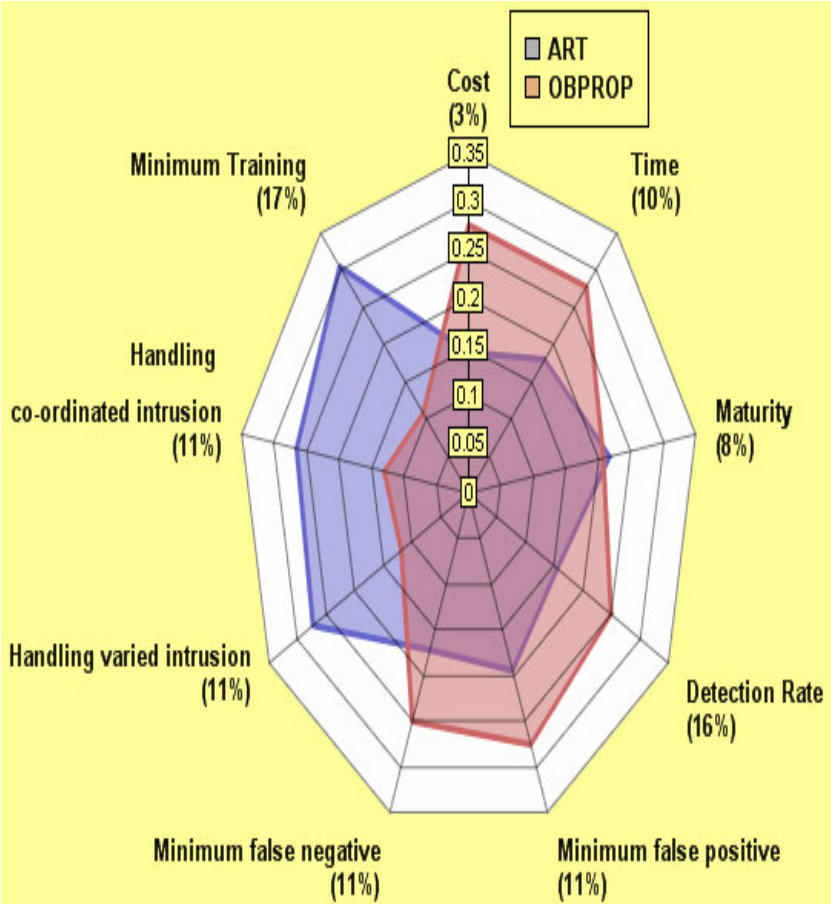

Figure 2. ART vs. OBPROP.

information obtained from previous works (Dutta et al., 2004; Yatim et al., 2006; Ahmad et al., 2009a,b,c, 2010). 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 criteria performance are shown in Table 3. The sum of local weights is equal to 1 and sum of global weights is 0.39 (that is, the global weight of performance).

The weights of sub criteria adaptable are shown in Table 4. The sum of local weights is equal to 1 and sum of global weights is 0.14 (that is the global weight of adaptable).

The weights of sub criteria aptitude are shown in Table 4. The sum of local weights is equal to 1 and sum of global weights is 0.22 (that is, the global weight of aptitude).

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%, there arises the need of subjective judgment revision. In this analysis, the obtained ratio is < 10% hence, there is no inconsistency whatsoever.

Comparative analysis

The comparative analysis of neural networks (NNs) is shown in Figures 2 to 5.

Figure 2 shows a comparison between artificial neural networks such as online Backpropagation and ART. The ART NN is better in case of minimum training, handling co-ordinated and varied intrusion. However, it is not good in other cases such as time, maturity, detection rate, false positive and false negative.

Figure 3 shows a comparison between ART and RPROP NNs. The RPROP NN is better in case of performance (detection rate, min. false positive, min. false negative, handling) and adaptable (cost and time). However, it is not good in other cases such as minimum training, maturity, handling co-ordinated and varied intrusion.

Figure 4 shows a comparison between ART and SVM NNs. The ART NN is better in the case of performance (detection rate, min. false positive, min. false negative), minimum training and aptitude (handling co-ordinated and varied intrusion). However, it is not good in other cases such as adaptable (cost and time) and maturity, Figure 5 shows a comparison between ART and SOM NN. The SOM NN is preferable to ART in case of performance (detection rate, min. false positive, min. false negative, handling), adaptable (cost and time) and maturity. On another hand, the ART is preferable in aptitude (handling co-ordinated and varied intrusion) and minimum training.

RESULTS AND DISCUSSION

Results are obtained by the multi criteria software (AHP

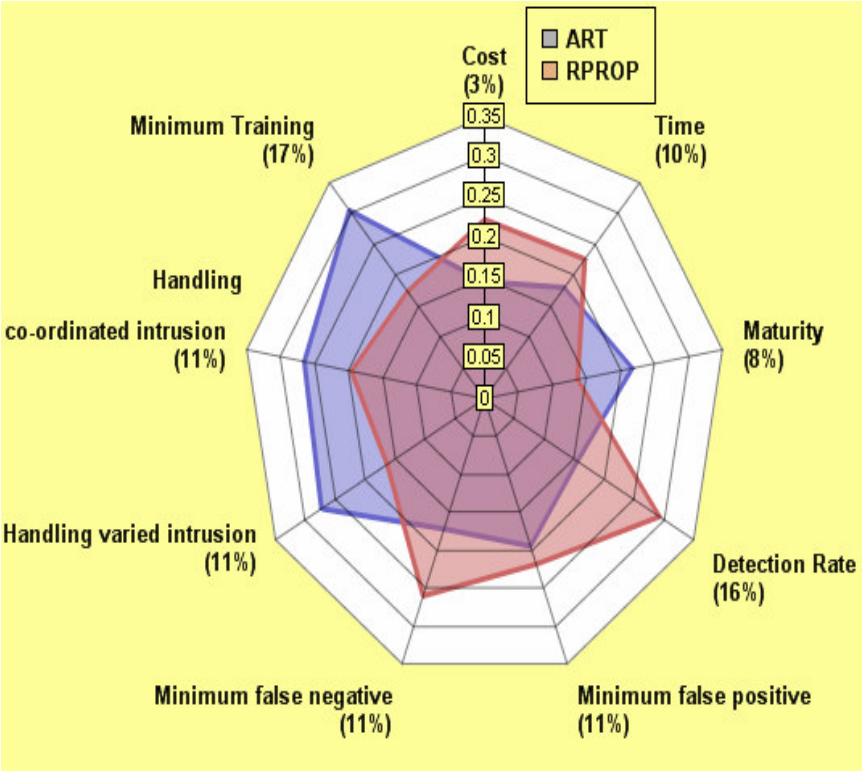

Figure 3. ART vs. RPROP.

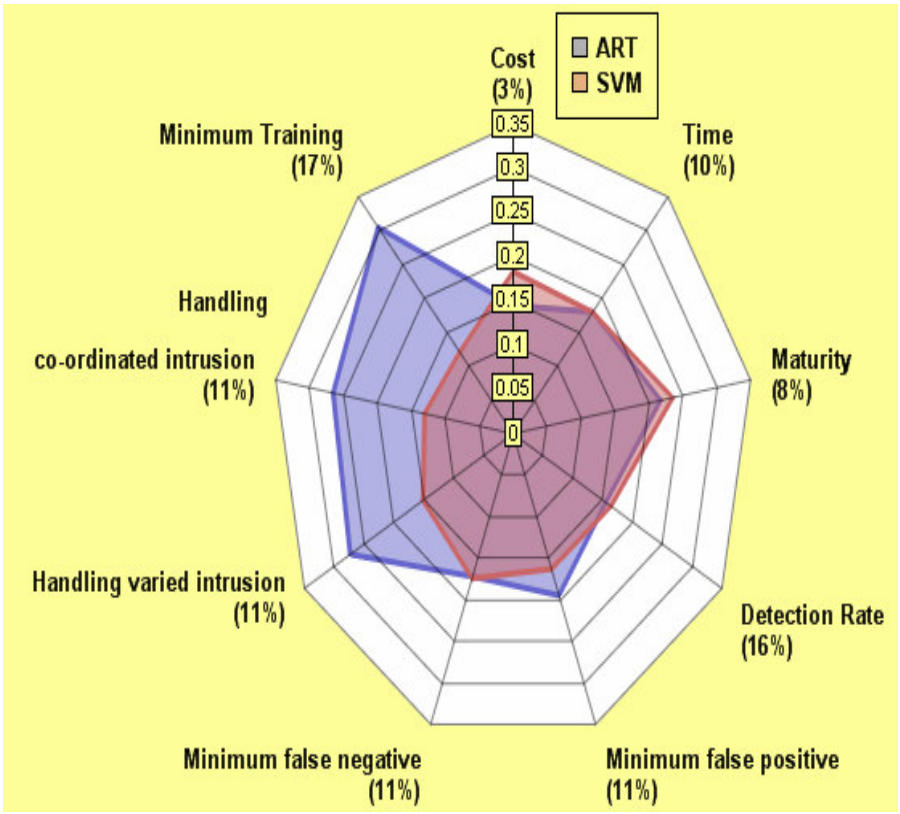

Figure 4. ART vs. SOM.

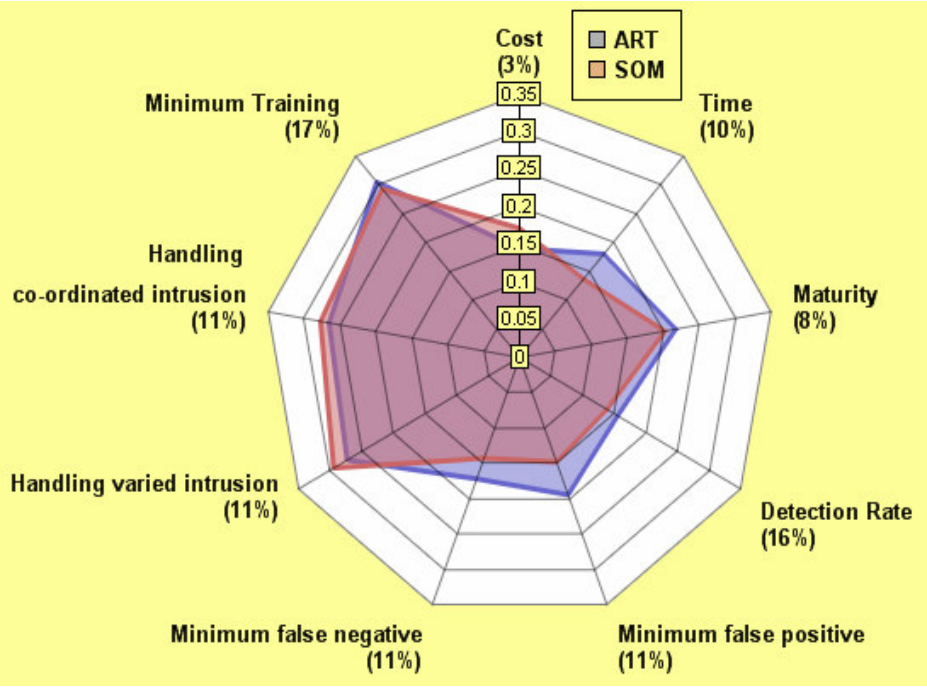

Figure 5. ART vs. SOM.

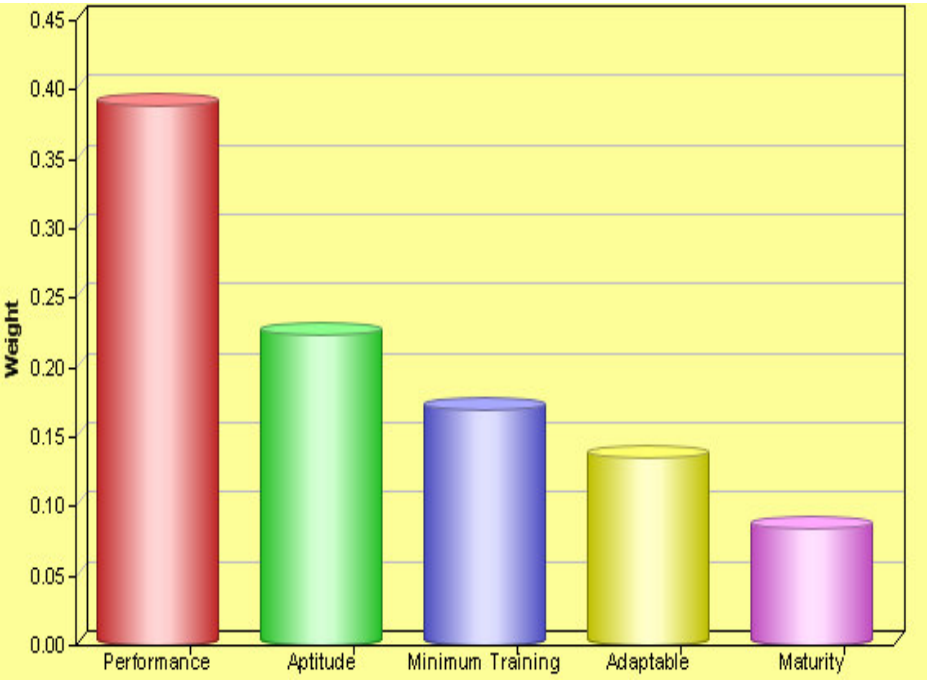

Figure 6. Criteria ranking.

project) and are presented in Figures 6 and 7.

Figure 6 indicates ranking among the criteria that are used in the evaluation of neural networks for intrusion detection. In this case, performance is ranked as first, aptitude as second, minimum training as third, adaptable as fourth and maturity as fifth in this work.

The ranking of alternatives such as SOM, ART, SVM, RPROP and BPROP is shown in Figure 7. Each

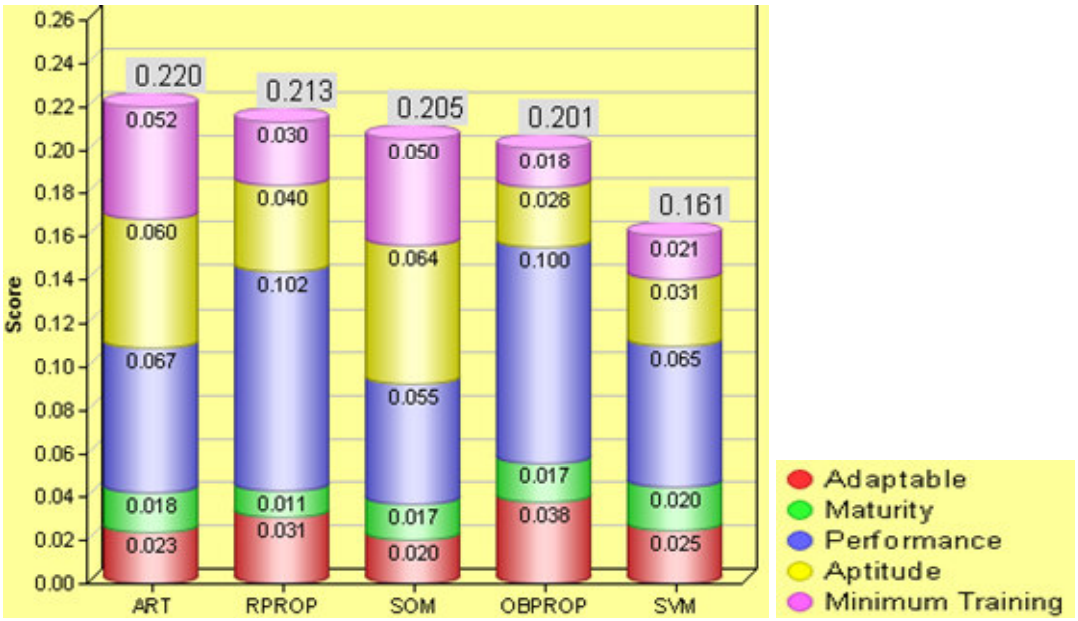

Figure 7. Alternatives ranking.

Table 6. Performance analysis based on weights.

Criterion	ART	RPROP	SOM	OBPROP	SVM
Performance (0.39)	0.07	0.10	0.06	0.10	0.07
Aptitude (0.22)	0.06	0.04	0.06	0.03	0.03
Minimum training (0.17)	0.05	0.03	0.05	0.02	0.02
Adaptable (0.14)	0.02	0.03	0.02	0.04	0.03
Maturity (0.08)	0.02	0.01	0.02	0.02	0.02
Total criteria weight (1.00)	0.22	0.21	0.21	0.20	0.16

alternative consists of five criteria as shown in different colours. The ART is ranked as first suitable NN to tackle present problems to intrusion detection. The red colour in ART alternative in Figure 7 represents a portion of adaptable (that is, 0.023 of the total criterion adaptable). The sum of all alternatives' adaptable value is equal to total adaptable value as shown in Figure 6.

Figure 7 shows the ranking of neural networks as evaluated in this work. Each NN is evaluated by five different criteria (adaptable, minimum training, performance, maturity and aptitude) and seven sub criteria (cost, time, detection rate, min. false positive, min. false negative, handling varied intrusion, handling coordinated intrusion).

The performance analysis based on weights is given in Table 6, which indicates each criterion value and its fraction in each alternative such as ART, RPROP, SOM, OBPROP, and SVM.

The obtained results demonstrate that in some cases, supervised NNs are better as compared to unsupervised NNs and vice versa. The results reflect that the use of hybrid or combination of neural network approaches (e.g. BPROP and SOM) in intrusion detection systems will enhance the security of computer and network systems.

Conclusion

In this paper, we evaluated five different neural networks for intrusion detection mechanism such as SOM, ART, SVM, OBPROP and RPROP using MCDM. The evaluation is based on two types of criteria, that is, the main criteria and sub criteria. The main criteria consists of adaptable, minimum training, performance, maturity and aptitude, on the other hand, the sub criteria consist of detection rate, minimum false positive, minimum false negative, cost, time, handling co-ordinated and varied intrusion. We concluded that the combined (hybrid) approach using artificial neural network is a more suitable tactic among other approaches to tackle the present

issues of intrusion detection systems such as regular updating, detection rate, false positive, false negative, and flexibility.

Future work

More research is needed to develop an optimized intrusion detection mechanism, which can identify network activity in a robust way. In this context, we will explore the possibility towards the application of artificial neural networks for intrusion detection that will have a better performance as compared to other approaches.

REFERENCES

Ahmad I, Abdullah AB, Alghamdi AS (2009a). Application of Artificial Neural Network in Detection of DOS Attacks. 2nd ACM international conference SIN '09: 229-234.

Ahmad I, Abdullah AB, Alghamdi AS (2009b). Application of Artificial Neural Network in Detection of Probing Attacks. 2nd IEEE Symposium on Industrial Electronics and Applications (ISIEA), pp. 557-562.

Ahmad I, Abdullah AB, Alghamdi AS (2010). Evaluating Intrusion Detection Approaches Using Multi-criteria Decision Making Technique. IJISCE, 1(1): 60-67.

Ahmad I, Abdullah AB, Alghamdi AS (2009c). Artificial Neural Network Approaches to Intrusion Detection: A Review. Telecommunications and Informatics conference (TELE-INFO'09), pp. 200-205.

Alghamdi AS (2009). Evaluating Defense Architecture Frameworks for C4I System Using Analytic Hierarchy Process. J. Comput. Sci., 5(12): 1078-1084.

Atthirawong W, McCarthy B (2002). An application of the analytical hierarchy process to international location decision-making. 7th Annual Cambridge International Manufacturing Symposium: Restructuring Global Manufacturing, University of Cambridge, UK, pp. 1-18.

Berrittella M, Certa A, Enea M, Zito P (2007). An Analytic Hierarchy Process for the Evaluation of Transport Policies to Reduce Climate Change Impacts. (Milano):http://www.feem.it.

Bhushan N, Kanwal R (2004). Strategic Decision Making: Applying the Analytic Hierarchy Process. Springer-Verlag, pp. 171-178.

Chien CC (2010). A Combined MCDM and Fuzzy MCDM Approach to Selecting the Location of the Distribution Center in the Hub Port: An Empirical Study on Hong Kong, Shanghai and Kaohsiung. IJICIC, 6(7): 3037-3051.

Denning D (1987). An Intrusion-Detection Model, IEEE Transactions on Software Engineering, SE-13(2).

Dey PK (2003). Analytic hierarchy process analyzes risk of operating cross-country petroleum pipelines in India. Nat. Hazards Rev., 4(4): 213-221.

Dutta M, Chatterjee A, Rakshit A (2004). A Resilient Backpropagation Neural Network based Phase Correction System for Automatic Digital AC Bridges. IEEE Precision Electromagnetic Measurements Digest, 374-375.

Forman EH, Gass SI, (2001-07). The analytical hierarchy process-an exposition. Oper. Res., 49: 469-487.

Grandzo JR (2005). Improving the faculty selection process in higher education. A case for the analytic hierarchy process. IR Applications: http://airweb.org.

Kunio S, Junzo W, Yoshiyuki Y (2009). Fuzzy AHP Approach to Comparison of Grant Aid for ODA in Japan. Int. J. Innov. Comput. Inf. Control., 5(6): 1539-1546.

Latifur K, Mamoun A, Bhavani T (2007). A new intrusion detection system using support vector machines and hierarchical clustering. The VLDB J., 16(4): 507-521.

James M (2005). The analytic hierarchy process. MSDN Magazine: http://msdn2.microsoft.com/.

Min L, Wang D (2009). Anomaly Intrusion Detection Based on SOM, WASE Int. Conference Inf. Eng., pp. 40-43.

Morteza A, Rasool J, Hamid RS (2006). RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks, Comput. Security, 25(6): 459-468.

Saaty TL (2000a). Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process. 2nd edition, RWS Publications, pp. 478-484.

Saaty TL, Shih HS (2009b). Structures in decision making. Eur. J. Operat. Res., 199(3): 867-872.

Steiguer De, Jennifer JE, Duberstein, Vicente L (2003). The analytic hierarchy process as a means for integrated watershed management. 1st Interagency Conference on Research on the Watersheds, pp. 736-740.

Yatim AHM, Utomo WM (2006). Efficiency Optimization of Variable Speed Induction Motor Drive Using Online Backpropagation. IEEE International Conference Power and Energy, PECon '06:, pp. 441-446.