Performance Evaluation of the Fuzzy ARTMAP for Network Intrusion Detection

Nelcileno Araújo[1], Ruy de Oliveira[2], Ed' Wilson Tavares Ferreira[2], Valtemir Nascimento[2], Ailton Shinoda Akira[3], and Bharat Bhargava[4]

[1] Universidade Federal de Mato Grosso - UFMT, Cuiabá, MT, Brasil
[2] Instituto Federal de Educação, Ciência e Tecnologia do Estado de Mato Grosso - IFMT, Cuiabá, MT, Brasil
[3] Universidade Estadual Júlio de Mesquita Filho - UNESP, Ilha Solteira, SP, Brasil
[4] Purdue University, West Lafayette, IN, USA
nelcileno@yahoo.com.br,
{ruy,ed,valtemir.nascimento}@cba.ifmt.edu.br,
shinoda@dee.feis.unesp.br, bb@cs.purdue.edu

Abstract. Recently, considerable research work have been conducted towards finding fast and accurate pattern classifiers for training Intrusion Detection Systems (IDSs). This paper proposes using the so called Fuzzy ARTMAT classifier to detect intrusions in computer network. Our investigation shows, through simulations, how efficient such a classifier can be when used as the learning mechanism of a typical IDS. The promising evaluation results in terms of both detection accuracy and training duration indicate that the Fuzzy ARTMAP is indeed viable for this sort of application.

Keywords: Fuzzy ARTMAP, security, intrusion detection.

1 Introduction

The non-authorized access into a computer network represents one of the most dangerous threats to the computer's security in such networks. Because of that, it is crucial to have mechanisms that inform system administrators of potential threats so proper actions can be taken, preventing the attacked system from further damage. These mechanisms are commonly called Intrusion Detection System (IDS).

In general, An IDS works based on one of two principles. It can either match suspicious patterns to previously known intrusion rules or recognize abnormal activities in the network [1]. The former approach is called *signature detection*, while the latter is the *anomaly detection*.

The drawback of signature-based IDSs is that they are limited to previously known attacks, i.e., these IDSs are not able to detect new forms of attacks that may arise. Because of that, new approaches, based on learning machine techniques, for anomaly detection are of paramount importance these days. Additionally, such techniques should not be too computationally intensive [2]. In this sense, we focus on the learning machine paradigm in this work.

S.M. Thampi et al. (Eds.): SNDS 2012, CCIS 335, pp. 23–34, 2012.

We investigate here the effectiveness of using the neural network called fuzzy ARTMAP in training an IDS. This classifier provides a unique solution known as stability-plasticity dilemma since it both preserves the previously acquired knowledge over the evaluated data (stability) and self-adapts to new patterns of classification (plasticity) [3]. Firstly, we evaluated the IDS training duration, global detection rate, and accuracy by using the well-known KDD99 training dataset. We used this dataset because it has been widely and successfully used for IDSs calibration [4]. Subsequently, we evaluated the IDS on a real wireless network (WLAN). In these experiments, four types of attackes were evaluated and the results were compared to three distinct IDS of the literature. The results are encouraging.

The remainder of this paper is organized as follows. In section 2 we present related work. Section 3 explains the fuzzy ARTMAP. In section 4 we introduce our proposed approach for training IDSs on the basis of the fuzzy ARTMAP, and also present the performance evaluations related to both the KDD99 dataset and the real WLAN. Finally in the last section we conclude our evaluations and outline potential future work.

2 Related Work

There exist various learning approaches for training and classifying IDS. The proposal presented in [5] shows that the Fuzzy ARTMAP classifier renders low performance in detecting intrusion. Nevertheless, their experiments were conducted in wired networks only and they did not use any optimizing mechanism to improve the right classification rate.

On the other hand, the proposal in [2] uses a genetic algorithm based technique, as optimizing mechanism, for computing setup parameters that enhance the effectiveness of the Fuzzy ARTMAP classifier toward 100% of correct detection rate. The disadvantage here is that the dataset used does not represent a wireless network either.

The work in [6] uses a Fuzzy ARTMAP neural network to detect intrusion in heterogeneous wireless networks. Their approach attempts to reduce error in classifying the attacks by using an access control security service based on the context aware role paradigm. As the proposal focuses on access control modeling, it does not fit Wireless LAN (WLAN) attacks.

Finally, in this work we propose a Fuzzy ARTMAP neural network as a classifier of features to recognize attacks in the MAC sub layer of a WLAN.

3 Fuzzy ARTMAP Neural Networks

Neural networks have been used extensively for detecting intrusions in computer networks [2], which confirms that the paradigm of learning by sampling in training IDSs are becoming more and more popular these days. In particular, the fuzzy ARTMAP neural network represents a valuable supervisioned learning system that classifies input data into stable categories to respond to random input patterns [3].

Fig. 1 depicts the architecture of the fuzzy ARTMAP neural network. It comprises two modules: fuzzy ART_a and fuzzy ART_b. Both modules use the same structure of

the neural network ART1 (not shown in the figure) that uses the logical operations of the fuzzy logic theory [7].

These two modules are interconnected by a third module called inter-ART which controls the training of the mapping of ART_a recognition categories onto ART_b recognition categories. The inter-ART associates the input parameters (ART_a) with the output parameters (ART_b) using the *match tracking* mechanism, aiming at maximizing the generalization of the recognition categories and minimizing the network errors [3].

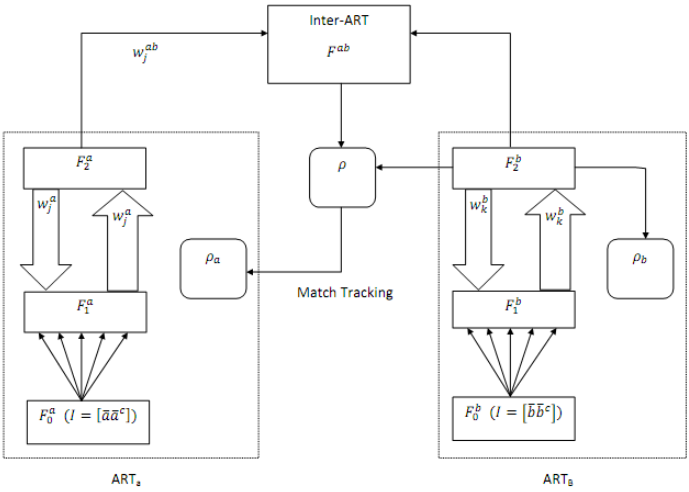


Fig. 1. Architecture of the fuzzy ARTMAP neural network [3]

The algorithm of such a neural network works based on the following steps [3]:

- **Step 1**: If needed, normalize the ART_a (input vector) and ART_b (output vector). Initially, all neuron values should be normalized to guarantee that they are in the range 0-1;
- **Step 2**: Encode the vectors of ART_a and ART_b modules: a new input pattern should go through a preliminary complement coding in order to preserve the information amplitude;
- **Step 3**: Initialize the weights and parameters of ART_a, ART_b and Inter-ART. First initialize the weights (when set to 1, means that all the categories are deactivated), then the training rate (β between 0 and 1), followed by the choice parameter ($\alpha > 0$) and finally the vigilance parameter (ρ_a, ρ_b and ρ_{ab} between 0 and 1);
- **Step 4**: Choose the category for ART_a and ART_b. If more than one module is active, take the one that has the highest ordering index;
- **Step 5**: Test the vigilance of ART_a and ART_b. If the vigilance criterion is met, then the resonance (match) takes place. Otherwise a new index is chosen restarting from phase 4. The searching process repeats until an index value, that meets the vigilance test, is found;

- **Step 6**: *Match tracking* between ART_a and ART_b: check if there was matching between the input and output. If not, search another index that satisfies it;
- **Step 7** Adaptation of the weights: the vector (layer F_2) of the ART_a, ART_b and Inter-ART are updated with the new weights;
- **Step 8**: Repeat steps 4 through 7 for every pair of vectors to be trained.

4 Investigating the Performance of the Fuzzy ARTMAP in Detecting Intrusions

In this section we will initially detail the use of the fuzzy ARTMAP classifier being used for training an IDS. In these evaluations, we used the well-known KDD99 training dataset. Subsequently, we will compare our approach with existing work in terms of its accuracy to detect attacks in real wireless LAN.

4.1 Applying Fuzzy ARTMAP Classifier on KDD99 Dataset

Despite being relatively old and encompasses just little attacks against UNIX based systems and Cisco routers, KDD99 [8] is a well-known dataset widely used in training and testing IDSs in the literature. Many researchers still adopt such a dataset for evaluating both intrusion detection and machine learning algorithms [4]. By using KDD99, we intended mainly to facilitate comparisons to similar work [1,2,9]. In fact, in order to reduce the amount of samples to be processed, we used here the so called training dataset (10% KDD99) only.

The input vector receives the registers of the KDD99 training dataset. However, we used the optimized dataset proposed in [9], in which only the most relevant features of the original dataset are taken. As a result, the input vector is shortened to a dimension of 14.

The output vector, which contains the classes of detections by the IDS, is defined through a binary coding of two bits, as illustrated in Table 1.

Table 1. Output Vectors (binary) corresponding of the classes of intrusions

Detection type	Class	Output vector *b*
Normal	S1	01
Anomaly	S2	10

To evaluate the performance of the IDS trained with the fuzzy ARTMAP classifier, we worked with three scenarios as shown in Table 2. Scenario 2 has half of the samples for effective training, and the other half for testing the Fuzzy ARTMAP. Scenarios 1 and 3 vary the amount of such samples. The idea here is to see how much such the variation of the number of samples impact the proposed approach performance. The whole dataset used in these evaluations contains 125.793 instances.

The parameters setup used in the fuzzy ARTMAP classifier for training the IDS are the same as the one in [10]. The reasoning here is that although the work in [10]

Table 2. Configuration of the simulated scenarios

Scenario	Total registers of the KDD99 training dataset in each phase	
	Training	Test
1	33%	67%
2	50%	50%
3	66%	34%

uses a neuro-fuzzy-wavelet network to detect voltage anomalies in electric power systems, the final goal is pretty similar to the one in our work. That is, both researches pursue to detect anomalies using data from a given dataset. Hence, we used as parameters setup for the fuzzy ARTMAP the values shown in Table 3.

Table 3. Configuration parameters for the Fuzzy ARTMAP classifier

Parameter	Value
Choice Parameter (α)	0,001
Training rate (β)	1
Network vigilance Parameter ARTa(ρ_a)	0,99
Network vigilance Parameter ART_b(ρ_b)	0,9
Vigilance Parameter of the inter-ART(ρ_{ab})	0,99

The efficiency of the IDS were assessed through the following parameters: training duration, global detection rate, accuracy rate.

The simulations were conducted using the WEKA programing tool [11], which had been used in [9] and turned out being very efficient in the implementation of patterns classifiers.

The results in Table 4 indicate that for the training duration parameter the three scenarios provided similarly small values, i.e., duration of about 2 minutes long. This happens mainly due to the stability-plasticity dilemma property of the classifier, which causes it to employ an incremental learning. This means it only trains new activity patterns, as it keeps the former learned activities (sort of retentive memory).

Based on that, as long as the new samples inserted into the dataset do not represent new activity patterns, no further training is needed. As a consequence, shorter training periods are achieved.

Another important observation to be highlighted in Table 4 is that the slight reduction in the training duration for the scenario 2 was not maintained for scenario 3. In other words, despite the gradual increase in the number of training data from scenario 1 to scenario 3, there was not a sensible plasticity in the learning achievement since the training duration reduction was not linear.

Table 4. Results of the Simulated Scenarios

Scenario	Performance	
	IDS training duration (sec)	Global detection rate (%)
1	122,97	72,85
2	118,81	87,20
3	121,54	88,91

Concerning the global detection rate parameter, one can see in Table 4 that from scenario 2 onwards the value of this parameter seems to converge to a value around 88%. This happens because of the reduction in the number of new activity patterns. It means that even though the number of samples in the training dataset have been increased, the sample contains no new learning categories.

The results depicted in Fig. 2 indicate that when the IDS input data includes a large diversity of values, it is possible to achieve higher accuracy rates. This is confirmed by the results for scenarios 2 and 3, in which at least 50% of the dataset are used for training the IDS, and an accuracy of approximately 90% is achieved. This is definitely an encouraging result given the short duration of the involved training.

In addition to the parameters addressed above, it is also very important to evaluate the false positive rate, since it might assist us in finding situations in which a classifier enhances detection rate at the expense of the accuracy [9].

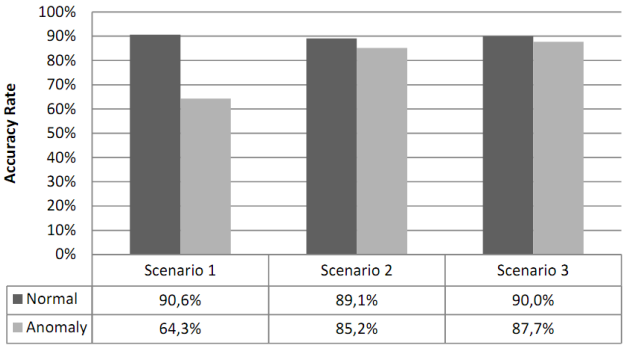


Fig. 2. Results of the accuracy rate for the simulated scenarios

As shown in Fig. 3, the neuro-fuzzy classifier did not perform satisfactorily for scenario 1 in which the training dataset used was limited to only 33% of the whole training dataset. In this case, almost half of the evaluated "normal data" were labeled as being anomalous data. On the other hand, as the number of samples in the training dataset increased the false positive rate reduced and established around 10%. Hence, it is proper to say that the accuracy of the classifier depends strongly on the threshold established for the minimal number of samples in the training.

The main advantage of the evaluated classifier shown in our evaluations is the fast processing in the training phase of the IDS. Even when a large number of samples were used (about 85.000 samples) the training duration was really short. Once again, this is possible because the fuzzy ARTMAP classifier keeps its former learned knowledge and only retrain the IDS when a new activity pattern comes in.

This property is key here since most classifiers have to train the whole training data whenever new samples are inserted in the dataset. The only problem here is that such a retraining may be complicated since changes can occur while the data are being retrained. Besides, when a new pattern is learned, there is no guarantee that the network topology and the previous learning parameter continue representing a good

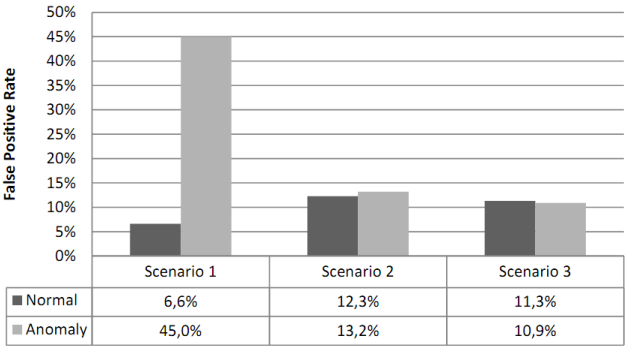


Fig. 3. Results of the false positive rate for the simulated scenarios

solution. As a consequence, the training duration increases because new decision regions are needed, the network will have more hidden layers, and the size of the neural network input matrix will be greater.

4.2 Applying Fuzzy ARTMAP Classifier on a WLAN

In order to validate our Wireless IDS (WIDS), we conducted evaluations in a controlled environment, whose topology is illustrated in Fig. 4, to generate data set to be used in training, validating and test of the WIDS. The evaluated network was composed of three wireless station and one access point (AP). Station 1 injected normal traffic into the network (HTTP, FTP). Airplay tool was executed in station 2 to launch simultaneously the four predefined attacks (chopchop, duration, deauthentication e fragmentation). In station 3 was run the wireshark to capture the passing-by (normal and intrusion) traffic. The predefined attacks are as follows:

- Chopchop – attacker intercept a cryptography frame and uses the base station to guess the clear text of the frame by brute force that is repeated until all intercepted frames are deciphered [12].
- Deauthentication - attacker transmits to the client stations a false deauthentication frame to render the network unavailable [13].
- Duration - attacker sends a frame with the high value of NAV (Network Allocation Vector) field to prevent any client station from using the shared medium to transmit [13].
- Fragmentation - attacker uses a fragmentation/assembly technique running in the base station to discover a flow key used to encrypt frames in a WLAN [12].

Next, the captured data were pre-processed to extract only the MAC header out of the control frames of the MAC sub layer (*protocol version*, *type*, *subtype*, *to DS*, *from DS*, *more fragment*, *retry*, *power management*, *more data*, WEP, *order*, *duration*, *address1*, *address2*, *address3* e *sequence control*). This was necessary because we intended to determine the impact of such frames in specifying the signatures of attacks against wireless LANs.

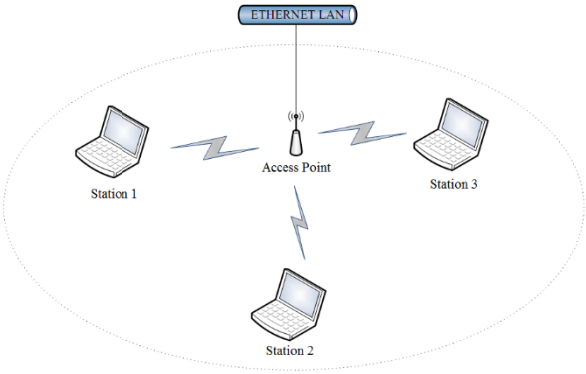


Fig. 4. Topology of the WLAN used for generating data

Subsequently, it was included in each sample a field with its type of attack so the classifier could distinct among training, validation and test frames. This way, it was simple to compare the detection by our algorithm against the actual cause of attack associated to that frame.

The generated data set collected in the experiments was divided in three subsets: training, validation and test. Table 5 shows how the samples were divided into both the three subsets and the recognition categories (type de traffic) evaluated in the experiments.

The generated data set collected in the experiments was divided in three subsets: training, validation and test. Table 5 shows how the samples were divided into both the three subsets and the recognition categories (type de traffic) evaluated in the experiments.

The training subset, as shown in Table 5, comprises 9600 samples: 6000 samples of normal traffic and 3600 samples of intrusion traffic. This subset is used to train the Fuzzy ARTMAP neural network to recognize these classification standards by adjusting dynamically the network parameters (vigilance, choose and training), mitigating the error rate between the expected output and the output computed by the network. The training is stopped once the error rate reaches a given limit.

Table 5. Distribution of the samples collected from the WLAN into datasets

			Datasets		
			Training	Validation	Test
Intrusion Categories of WIDS	Normal		6000	4000	5000
	Intrusion	ChopChop	900	600	800
		Deauthentication	900	600	800
		Duration	900	600	800
		Fragmentation	900	600	800
Total Number of Samples			9600	6400	8200

The validation of the Fuzzy ARTMAP neural network occurs by using validation data set composed of 6400 samples, being 4000 samples of normal traffic and 2400 samples of intrusion traffic, as shown in Table 5. The validation phase is needed to prevent that, in some cases, the classifier presents a good performance with the samples from the training subset, but keeps a poor performance with samples from the test subset.

Once the network is trained and validated, we get the parameters of the Fuzzy ARTMAP neural network, which are: choose parameter (α) = 0.01, vigilance parameter of the network ARTa (ρ_a) = 0.7, vigilance parameter of the network ARTb (ρ_b) = 1, vigilance parameter of the associative map (ρ_{ab}) = 0.99 and training rate (β) = 1. After this, the test subset is computed by the classifier which computes its outputs. From Table 5, the test subset has 8200 new samples divided in 5000 samples of normal traffic and 3200 samples of intrusion traffic.

In the evaluation of our approach, we compared our results with the ones of other three classifiers: Support Vector Machine (SVM), Multilayer Perceptron with Backpropagation (MPBP) and Radial Basis Function (RBF). We used here the test subset presented in Table 5. These classifiers were chosen because of their large use in machine learning based IDS [5].

The following metrics can be used to evaluate a pattern classifier for intrusion detection systems: True Positive (TP), an intrusive activity is identified correclty; True Negative (TN), a non-intrusive activity is identified correctly; False Positive (FP), a non-intrusive activity is identified as an intrusive one; False Negative (FN), a intrusive activity is identified as an non-intrusive one.

In general, however, the detection rate and false alarm rate metrics are the most common ones in evaluating IDSs [4]. The detection rate is is computed as TP/(TP+FN) and false alarm rate is computed as FP)TN+FP). An efficient classifier should get a high detection rate and a low false alarm rate [4]. We present next the results from the performance evaluation we have conducted.

To evaluate the performance of the classifier of standard used in the proposed WIDS, 8200 samples of the test subset were used in the two comparison scenarios below.

The result for the first scenario, shown in Fig 5, we have the training time spent by the classifier in constructing its learning data set. It is clear that our approach renders much shorter training time than the others the classifiers. This is due mainly the stability-plasticity property [3] that causes the Fuzzy ARTMAP neural network to use incremental learning (training only the new standards of activities), without forgetting the standards of activities previously learned.

Fig. 6 shows the result of the second evaluated scenario, in which the detection rate of the classifiers are evaluated based on the categories above mentioned. Note that for the normal category, although our classifier gets a representative detection rate of roughly 80%, it performs poorer than the other classifiers.

Regarding the categories related to attacks, we have two clearly distinct situations. The four classifiers provided high detection rate of approximately 100% for the duration and deauthentication attacks. This means these categories of attacks have traffic characterization of easy recognition by the classifiers evaluated in this work.

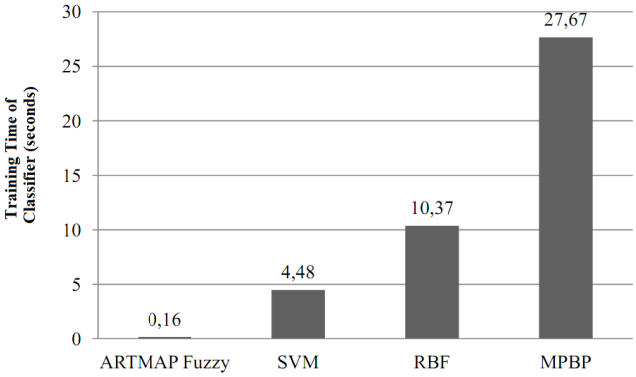
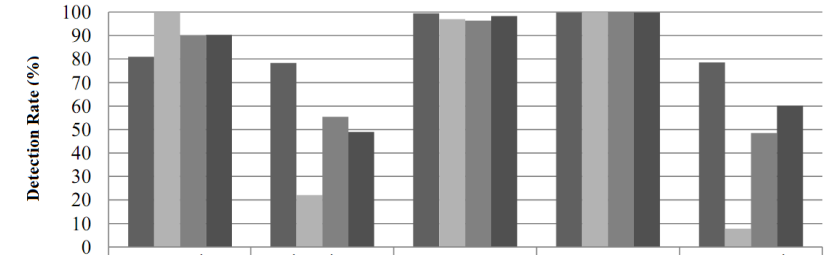


Fig. 5. Training time for the classifiers



	Normal	ChopChop	Deauthentication	Duration	Fragmentation
ARTMAP	81	78,3	99,5	99,8	78,6
SVM	99,9	22,1	97	99,8	7,8
RBF	89,9	55,4	96,3	100	48,5
MPBP	90,3	49	98,3	99,8	60,1

Fig. 6. Detection rate for the classifiers

On the other hand, ChopChop attacks and Fragmentation are harder to detect, since their signature are too similar to the normal category. Even so, the Fuzzy ARTMAP outperformed the other three classifiers, as it provided detection rate near 80%, while the other classifiers managed rates in the range 7.8% to 60%.

4.3 Discussions

From the results obtained in this work, it is sensible to say that there are rooms for improvements in this application of the fuzzy ARTMAP. The evaluation of the proposed WIDS along with the other three approaches indicates that Fuzzy ARTMAP neural network helps reducing training time and additionally provides high detection rate. The main issue to be addressed is to find a fine balance between high accuracy rate and low false positive rate. We believe this can be reached by using the neuro-fuzzy classifier evaluated here in conjunction with other low computational processing schemes like wavelet, rough sets or genetic algorithms.

5 Conclusions and Outlook

We have evaluated the efficiency of the fuzzy ARTMAP classifier in assisting an IDS. The achieved results suggest that this classifier is viable to be implemented in anomaly-based IDSs. Using short period of training resulted in high detection and accurate rates. In the preliminary evaluations conducted here, by comparing our proposal with the existing ones, our approach performed really well.

As future work, we intend to investigate the use of the fuzzy ARTMAP classifier in hybrid training architectures. This means to combine this classifier with other lightweight classification techniques. Another interesting task to be conducted is to apply new feature selection techniques towards further reducing the vectorial space of the samples used in the IDS training. The challenges ahead regard achieving these enhancements without compromising accuracy and/or the computational processing.

Acknowledgments. This material is based on a research project funded by the Foundation for Research Support of Mato Grosso (FAPEMAT) on the supervision of the Network and Security Research Group (GPRS). GPRS is managed by the Federal Institute of Mato Grosso (IFMT) in conjunction with the Federal University of Mato Grosso (UFMT), State University Júlio de Mesquita Filho (UNESP) and Federal University of Uberlandia (UFU). The authors acknowledge the facilities provided by IFMT for the development of this work.

References

1. Souza, P.: Study about anomaly based intrusion detection systems: an approach using neural networks. M.Sc. Thesis, Salvador University/Salvador (2008)
2. Vilakazi, C.B., Marwala, T.: Application of feature selection and fuzzy ARTMAP to intrusion detection. In: Proceedings of 2006 IEEE International Conference on Systems, Man and Cybernetics, pp. 4880–4885 (2006)
3. Carpenter, G.A., Grossberg, S., Markuzon, N., Reynold, J.H., Rosen, D.B.: Fuzzy ARTMAP: A neural network for incremental supervised learning of analog multidimensional maps. IEEE Transactions on Neural Network 3(5), 689–713 (1992)
4. Wu, S., Banzhaf, W.: The Use of Computational Intelligence in Intrusion Detection Systems: A Review. Applied Soft Computing 10, 1–35 (2010)
5. Ahmad, I., Abdullah, A., Alghamdi, A.: Towards the selection of best neural network system for intrusion detection. International Journal of the Physical Sciences 5(12), 1830–1839 (2010)
6. Santra, A.K., Nagarajan, S., Jinesh, V.N.: Intrusion Detection in Wireless Networks using FUZZY Nerural Networks adn Dynamic Context-Aware Role based Access Control Security (DCARBAC). Int. Journal of Computer Application 39(4), 23–31 (2012)
7. Carpenter, G.A., Grossberg, S., Rosen, D.B.: Fuzzy ART: fast stable learning and categorization of analog patterns by an adaptive resonance system. Neural Networks 4(1), 759–771 (1991)
8. Lippmann, R., Haines, J.W., Fried, D., Korba, J., Das, K.: The 1999 DARPA off-line intrusion detection evaluation. Computer Networks 34(4), 579–595 (2000)

9. Araújo, N., Shinoda, A.A., de Oliveira, R., Ferreira, E.T.: Identifying important characteristics in the KDD99 intrusion detection dataset by feature selection using a hybrid approach. In: Proceedings of 2010 IEEE International Conference on Telecommunications, pp. 552–558 (2010)
10. Malange, F.C.V.: A neuro-fuzzy-wavelet network to detect voltage anomalies in electric power systems. D.Sc. Thesis. Universidade Estadual Júlio de Mesquita Filho/Ilha Solteira (2010)
11. Bouckaert, R.R., et al.: WEKA manual for version 3-7-0, `http://www.cs.waikato.ac.nz/ml/weka/` (last access: August 2009)
12. Bellardo, J., Savage, S.: 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In: Proceedings of the 12th Conference on USENIX Security Symposium, vol. 12, pp. 15–28 (2003)
13. Bittau, A., Handley, M., Lackey, J.: The Final Nail in WEP's Coffin. In: Proceedings of the 2006 IEEE Symposium on Security and Privacy, pp. 386–400 (2006)