**Kappa-Fuzzy ARTMAP: A Feature Selection**

**Based Methodology to Intrusion Detection in Computer Networks**

|  |  |  |  |
| --- | --- | --- | --- |
| Nelcileno Virgílio de Souza Araújo11Institute of ComputingFederal University of Mato GrossoCuiabá, MT, Brazilnelcileno@yahoo.com.br | Ruy de Oliveira2Ed’Wilson Tavares Ferreira4Valtemir Emerêncio do Nascimento52,4,5Department of InformaticsFederal Institute of Mato GrossoCuiabá, MT, Brazil{ruy,ed,valtemir}@cba.ifmt.edu.br | Ailton Akira Shinoda33Department of Electrical EngineeringState University Júlio de Mesquita FilhoIlha Solteira, SP, Brazilshinoda@dee.feis.unesp.br | Bharat Bhargava66Department of Computer SciencePurdue UniversityWest Lafayette, IN, USAbbshail@purdue.edu |
|  |  |  |

**Abstract –Intrusions in computer networks have driven the development of various techniques for intrusion detection systems (IDSs). In general, the existing approaches seek two goals: high detection rate and low false alarm rate. The problem with such proposed solutions is that they are usually processing intensive due to the large size of the training set in place. We propose a technique that combines a fuzzy ARTMAP neural network with the well-known Kappa coefficient to perform feature selection. By adding the Kappa coefficient to the feature selection process, we managed to reduce the training set substantially. The evaluation results show that our proposal is capable of detecting intrusions with high accuracy rates while keeping the computational cost low.**

**Keywords: feature selection, Kappa coefficient, Fuzzy ARTMAP neural network, intrusion detection**

# Introduction

Intrusion detection in computer networks represents an important step towards securing such systems from a variety of security related threats [1]. Novel techniques for Intrusion Detection Systems (IDSs) have emerged in recent years, and most of them aim at improving primarily the detection algorithm of these systems. As the volume of traffic in communication networks has been increasingly growing, most existing approaches tend to suffer from performance inefficiency because, in such cases, they become processing intensive [1]. This problem is known as curse of dimensionality, where the amount of data collected from the network, to be processed, is too high that the IDS become ineffective.

It is crucial to extract from the training set the most representative features only, as long as they are sufficient to make it possible for effective attack detection. Feature selection is the technique used to reduce the dimension of the involved dataset [2]. Using this technique, only the really significant features, for defining a given profile, are kept in the dataset. The irrelevant ones, as well as the redundant data are discarded [3].

We can classify the feature selection algorithm into three methods: 1) FILTER, that uses an independent metric to compute the relevance of the features; 2) WRAPPER, that employs learning machines algorithms to obtain the optimal subset which contains only the really effective features; 3) EMBEDDED, that uses the FILTER method to select the candidate features from the training set and the WRAPPER method to evaluate the selected candidate features in the selection of the optimal subset [3].

We propose an approach that uses the fuzzy ARTMAP classifier [5] and the Kappa coefficient [4] to evaluate and extract, from the training set, the most relevant features towards the optimal subset which has two traffic profile only: normal and anomalous. The former concerns the traffic related to users who have permission to use the network, and the latter represents any traffic that is not considered normal.

The remainder of this paper is organized as follows. In section II we address related research. Section III describes our ideas, detailing the fuzzy ARTMAP neural networks and the Kappa coefficient concept. In section IV, the experiments, including the results, conducted with our proposed mechanism over the well-known KDD99 dataset [6] are presented. Section V provides observations and conclusions and outlines potential future activities.

# Related work

There has been a lot of research on feature selection for intrusion detection in computer networks. The research in [7], [8], [9] and [10] use the well-known KDDD99 [6] training set as the knowledge base.

In [7], the information gain is the key metric used in the feature selection algorithm to get the optimal subset. They use the decision tree as intrusion detection algorithm. The approach in [8] selects the most relevant features through the entropy. Subsequently, the k-means algorithm is used to join the registers of the optimal subset in five groups. These grouped registers are then used for training the hybrid classifier, based on naive bayes and k-nearest neighbor techniques, towards identifying intruders.

The ideas in [9] developed several learning machine strategies in a single IDS that comprised the k-means clustering technique, optimization by ant colony and support vector machine (SVM). The optimal features subset is obtained by applying the gradual features extracting algorithm. The approach proposed in [10] uses a multiclass classifier based IDS. Its architecture is based on three perspectives: 1) the entering traffic patterns are pre-processed and the redundant features are discarded, 2) a feature selection algorithm based on genetic algorithm is used to enhance the mitigation of the classifier computational complexity, 3) a neural tree model is used as a classification machine.

In the ideas for IDS in [7], [8], [9] and [10] one can see a trend in classifying the attacks in multi class mode, and also the use of serial learning machine. Our approach makes use of the Kappa coefficient as a metric of feature relevance. Besides, we gave priority to detecting anomalies in the training set. Identifying the exact sort of attacks is not a goal for us. We have two possible attack profiles: normal and anomaly. Hence, unlike the classification of multiple attacks, which identifies the exact type of attack at the cost of computational effort, our approach speeds up the IDS operation considerably [1], [2].

# Proposed approach to detect intruders

The concepts and mechanisms used in our approach to detect intrusions in computer networks is described below.

## *Feature Selection*

In complex pattern classification scenarios there might be redundant characteristics in the evaluated data, as the information may be present in more than one feature. Such a redundancy may raise the computational cost of the IDS and impact its accuracy [2]. Feature selection addresses this problem by reducing the training set towards a new feature subset, called optimal subset, which contains only the features that are indeed representative of the original dataset.

The strategy used is to search the features in the original dataset and is called Sequential Forward Search (SFS) [3]. As shown in Fig. 1, by this strategy, the training set is scanned recursively and at each iteration the most relevant feature is moved to the optimal subset. The algorithm stops when either the so called Kappa coefficient (detailed later) of the subset of candidates features reaches its threshold (Kappacurrent >= 1) or the currently computed coefficient is smaller than the previous one.

Actually, the relevance of a given feature is given by the Kappa coefficient just after its WRAPPER method applies the fuzzy ARTMAP neural network (detailed later) to assess the selected feature ability to perform good classification.

## *Fuzzy ARTMAP Neural Network*

The fuzzy ARTMAP classifier is a neural network for incremental supervised learning. It uses an adaptive resonance system to avoid restarting the training of the classifier for every new input pattern, and so it allows for keeping and extending the previously obtained knowledge [5].



Figure. 1. Flowchart of the proposed feature selection algorithm using SFS.

The architecture of fuzzy ARTMAP network consists of two modules: fuzzy ARTa and fuzzy ARTb. Both modules use the same structure of the neural network called ART1 which uses the logical operations of the fuzzy logic theory [11].

These two modules are interconnected by a third module called inter-ART that controls the mapping of the ARTa recognition categories onto ARTb recognition categories. The inter-ART associates the input parameters (ARTa) with the output parameters (ARTb) using the match tracking mechanism, aiming at both maximizing the generalization of the recognition categories and mitigating the network errors [5] [11].

The algorithm of such a neural network works based on the following steps [5] [11]:

**Step 1**: If needed, normalize the ARTa (input vector) and ARTb (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 ARTa and ARTb 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 ARTa, ARTb 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 (α > 0) and finally the vigilance parameter (ρa, ρb and ρab between 0 and 1);

**Step 4**: Choose the category for ARTa and ARTb. If more than one module is active, take the one that has the highest ordering index;

**Step 5**: Test the vigilance of ARTa and ARTb. If the vigilance criterion is met, then the resonance (match) takes place. Otherwise a new index is chosen restarting from step 4. The searching process repeats until an index value, that meets the vigilance test, is found;

**Step 6**: Match tracking between ARTa and ARTb: 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 of the ARTa, ARTb and Inter-ART are updated with the new weights;

**Step 8**: Repeat steps 4 through 7 for every pair of vectors to be trained.

## *Kappa Coefficient*

Using the fuzzy ARTMAP classifier to evaluate the features in the training set results in the so called confusion matrix [1]. This matrix tells us the number of correct classifications as well as the predicted ones by the classifier. The classifier performance is usually carried out based on the contents of this matrix. Table I is a representation of the confusion matrix for the intrusion detection problem.

TABLE I. Confusion Matrix For The Problem Of The Intrusion Detection

|  |  |  |
| --- | --- | --- |
|  | **Predicted Class** | **Total** |
| ***Negative Class (Normal)*** | ***Positive Class (Anomaly)*** |
| **Actual Class** | ***Negative Class (Normal)*** | True Negative (TN) | False Positive (FP) | l1 =TN+FP |
| ***Positive Class (Anomaly)***  | False Negative (FN) | True Positive (TP) | l2 =FN+TP |
| **Total** | c1 = TN+FN | c2 = FP+TP | Total of classified units (N) |

In our approach, the entries of the confusion matrix have the following meaning; True Positive (TP) – an intrusive activity is detected correctly; True Negative (TN) – a non-intrusive activity is correctly identified; False Positive (FP) – a non-intrusive activity is wrongly identified as an intrusive one; False Negative (FN) – an intrusive activity is wrongly classified as a non-intrusive one.

In order to evaluate the performance of the classifier in detecting intrusions, several metrics have been computed from the entries of the confusion matrix. In the area of intrusion detection system, the main metrics that have been used are as follows [1]:

* Detection rate ($\frac{TP}{FN+TP}$) – proportion of the correctly classified intrusive ativities;
* False alarm rate ($\frac{TN}{TN+FP}$) – proportion of the normal activities that are wrongly classified as intrusive ones;
* Accuracy ($\frac{TN+TP}{N}$) – proportion of the correct predictions;
* Precision ($\frac{TP}{FP+TP}$) – proportion of intrusive activities that are corrected classified.

We use an additional evaluation metric called Kappa coefficient which is seen as an agreement metric, first used by observers of the psychology area [4]. The key idea then was to use the Kappa coefficient to measure the level of agreement or disagreement of a group of people observing the same phenomenon [4].

As far as the intrusion detection problem is concerned, the Kappa coefficient k measures the proportion of observed agreement *Po* between the existing classes of behavior (actual class) and the predicted ones (predicted class). This is performed over the training set after the proportion of agreement expected by chance *Pa* has been removed. Equations (1), (2) and (3), show how the Kappa coefficient is calculated.

$k=\frac{P\_{o}-P\_{a}}{1-P\_{a}}$

$P\_{o}=\frac{TN+TP}{N}$

$P\_{a}=\frac{\left(c\_{1}\*l\_{1}\right)+(c\_{2}\*l\_{2})}{N}$

Once the Kappa coefficient *k* has been computed, its value defines how close the actual and predicted values are. Values of *k* close to zero indicate that the classified units occurred by change. On the other hand, values of *k* close to 1 means that the agreement between the two classes is quite high [4].

The main reason for using the Kappa coefficient, as the metric to select the most relevant features of the training set, as well as for evaluating the quality of the IDS classification, is that both the accuracy and precision metrics are improper to scenarios where the involved classes are not equally represented in the training set [12], as is the case here.

Table II shows such a situation, where the amount of normal samples in the training set represents 98% of the sample space, and only the remaining 2% correspond to the anomaly samples.

Note that in spite of a detection rate of 2%, the values for the accuracy and precision metrics indicate incorrectly the success of the classifier. Contrarily, the value computed for the Kappa coefficient clearly shows the classifier inefficiency. Obviously, the inefficiency here is related to the fact that practically all anomaly traffic (49) was misdetected as false negative outcome by the classifier, as shown in Table II.

TABLE II. Confusion Matrix And Evaluation Metrics For A Training Set With Heterogeneous Sample Space Divided Between The Classes Of Behavior

|  |  |  |
| --- | --- | --- |
|  | **Predicted Class** | **Total** |
| ***Negative Class (Normal)*** | ***Positive Class (Anomaly)*** |
| **Actual Class** | ***Negative Class (Normal)*** | 2450 | 0 | l1 = 2450 |
| ***Positive Class (Anomaly)*** | 49 | 1 | l2 = 50 |
| **Total** | c1 = 2499 | c2 = 1 | 2500 |

|  |
| --- |
| **Detection rate = 2%** |
| **False alarm rate = 0%** |
| **Accuracy = 98.04%** |
| **Precision = 100%** |
| **Kappa = 0.038** |

## *Proposed Model for Intrusion Detection System*

Fig. 2 depicts the block diagram of our strategy to detect intrusions. First, the data (S) are pre-processed, where the feature selection is conducted using the Kappa coefficient as the agreement metric, the fuzzy ARTMAP to assess the selected features and the SFS to generate the optimal subset (SW). After that, the intrusion recognition phase begins, in which the optimal subset is used to train the fuzzy ARTMAP. As a result, the activities presented to the classifier are grouped as traffic from the network clients (normal class) or traffic from malicious users (anomaly class). Afterwards, the IDS is evaluated with the test set (ST).



Figure 2. Block diagram of the proposed solution.

# Performance evaluations

In this section, we present the evaluation of the proposed strategy to detect intrusions. First we describe the methodology we used to assess our Kappa-fuzzy ARTMAP based solution, and then the experiments are presented and observations made.

## *Methodology*

In our experiments, we used the well-known KDD99 [6] dataset. Even though it is a relatively old dataset and encompasses little attacks against both UNIX systems and CISCO routers, this dataset is still largely used by researchers worldwide to evaluate not only intrusion detection algorithm but also learning machines algorithms [1]. Thus, using such a dataset facilitates comparison to related work.

Table III shows how KDD99 is organized in terms of contents. The 10%KDD99 subset, usually, plays the role of the training set in IDS evaluations, as it contains most of the samples related to intrusive activities. Obviously, this subset represents a condensed version of the complete dataset Whole KDD99 [6]. The Corrected KDD99 subset contains new attack patterns [6].

TABLE III. Classes Of Behavior Of The KDD99 Intrusion Detection Subsets In Terms Of Samples Amount

|  |  |  |  |
| --- | --- | --- | --- |
| **Dataset** | **Normal** | **Anomaly** | **Total of samples** |
| 10% KDD99 | 97277 | 396743 | 494020 |
| Corrected KDD99 | 60593 | 250436 | 311029 |
| Whole KDD99 | 972780 | 3925650 | 4898430 |

The training set used in these experiments contains 10.000 samples taken out of the 10%KDD99. These samples were taken considering the representativeness of the 22 classes of attacks, as well as that of the normal class (without attack).

To evaluate the proposed IDS performance we used the 10-fold cross-validation data partitioning method [13] on the training set. By this method, the dataset is partitioned in 10 subsets of 1000 samples each. At each iteration, one of the 10 subsets represents the test set and the 9 others represent the training set. The prediction accuracy is given by the average of the correctness percentage of the 10 iterations.

Table IV presents the parameters of the fuzzy ARTMAP classifier used in our approach to detect intrusions. The reasoning for such values is that, for a good classification decision, the neural network should be trained quickly (β=1) and the classifier should be well sensitive to variations in the input standard (ρ close to 1) [14].

TABLE IV. Setup 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 ARTb($ρ\_{b}$) | 0.9 |
| Vigilance parameter of the inter-ART($ρ\_{ab}$) | 0.99 |

All simulations were performed using the MATLAB [9] programming tool.

## *Results*

Once the training set is pre-processed by using the Kappa-fuzzy ARTMAP model, as shown in Fig. 1, the search for the optimal subset starts. Fig. 3 shows the outcome of SFS when evaluating all the 41 features of the pre-processed training set. Note that in this experiment, the SFS found the best result when it reached 3 features. By the algorithm shown in Fig. 1, the SFS would stop searching at this point. The evaluation of the remaining features, from 4 to 41 is kept for the sake of clarity only. Because of that, the term “candidate feature” is used in the figure.

The results in Fig. 3 show clearly the relevance of Kappa coefficient in the selection of the optimal subset. From 41 features in the training set, only three of them were needed in the optimal subset. That is, 38 features were simply discarded. In this particular case, the 3 features in the optimal subset were *logged in*, *dst bytes* and *src bytes*. This outcome implies substantial gain in terms of computational costs.

Table IV emphasizes the relevance of applying feature selection on the training set. By comparison, we note that the original dataset performed poorly than the pre-processed dataset. The false alarm rate using the optimal subset reduced over 50%. From these experiments, it is evident that a dataset without such a pre-processing work compromises the IDS detection capacity.

The comparison results of our proposal against the IDS architectures proposed in [7], [8], [9] and [10], are presented in Table V. The metrics used are detection rate, false alarm rate and accuracy. The outcome is quite encouraging, as our strategy, despite using much less features, performed similar to the others, in terms of intrusion detection. Besides, the accuracy of our strategy is the second best among all evaluated schemes. This is due to its high detection rate.

The main drawback of the Kappa-fuzzy ARTMAP is its false alarm rate that was outperformed by the other strategies. A possible reason for such inefficiency is that the classifier intrusion sensitivity is too high due to the used parameters setting in the fuzzy ARTMAP neural network.

TABLE IV. Performance Evaluation Of The fuzzy ARTMAP For 41 Features And The 3 Features Of The Optimal Subset.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Number of features** | **Detection rate (DR)** | **False alarm rate (FPR)** | **Accuracy** | **Precision** | **Kappa** |
| 41  | 98,79% | 5,91% | 97,86% | 98,54% | 0,9323 |
| 3 | 99,24% | 2,27% | 98,94% | 99,43% | 0,9667 |

TABLE V. Comparison Of Performance Among IDSs Based On Feature Selection.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Number of attributes** | **Detection rate (DR)** | **False alarm rate (FPR)** | **Accuracy** | **Precision** |
| J48[6] | 12 | 98,04% | 1,53% | 98,22% |
| K-means+K-NN+Bayes[7] | - | 98,18% | 0,83% | 99,00% |
| GFR[8] | 19 | 97,06% | 0,49% | 98,62% |
| NeuroTree[9] | 16 | 97,91% | 1,3% | 98,38% |
| Our proposal | 3 | 99,24% | 2,27% | 98,94% |

# conclusions

The evaluation results stress the viability of integrating Kappa with fuzzy ARTMAP for both feature selection and intrusion detection. The substantial reduction in the training set by the feature selection used spares crucial computational efforts. Additionally, the use of the Kappa coefficient as a concordance metric makes it possible the use of a condensed training set without affecting other IDS performance metrics.

For future work, we will investigate techniques to minimize the IDS false alarm rates. We intend to extend our intrusion detection ideas to other training set that include different network technologies such as wireless and mobile networks.

#

Figure 3. Subset of candidate features for each SFS iteration on the training set.

##### Acknowledgments

This material is based on a doctorate scholarship partially funded by the CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) on the supervision of Eletrical Engineering Program at State University Júlio de Mesquita Filho (UNESP). It is also partially funded by the Foundation for Research Support of Mato Grosso (FAPEMAT).

##### References

1. S. Wu and W. Banzhaf, “The Use of Computational Intelligence in Intrusion Detection Systems: A Review,” *Applied Soft Computing*, vol.10, p. 1-35, 2010.
2. Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, Wei-Yang Lin, “Intrusion detection by machine learning: A review,” *Expert Systems with Applications*, vol. 36, n. 10, pp. 11994-12000, 2009.
3. I. Guyon and A. Elisseeff, “An introduction to variable and feature selection,” *Journal of Machine Learning Research*, vol.3, pp.1157–1182, 2003.
4. J. Cohen, “A coefficient of agreement for nominal scales,” *Educational and Psychological Measurement*, vol. 20, no. 1, pp. 37-46, 1960.
5. G. A. Carpenter, S. Grossberg, N. Markuzon, J. H. Reynold & D. B Rosen, “Fuzzy ARTMAP: A neural network for incremental supervised learning of analog multidimensional maps,” *IEEE Transactions on Neural Network*, vol. 3, n. 5, pp. 689-713, 1992.
6. R. Lippmann, J. W. Haines*,* D. J. Fried, J. Korba & K. Das, “The 1999 DARPA off-line intrusion detection evaluation,” *Computer Networks*, vol.34, n.4, pp. 579-595, 2000.
7. A. Alazab, M. Hobbs, J. Abawajy, M. Alazab, "Using feature selection for intrusion detection system," in *Proceedings of* *International Symposium on* *Communications and Information Technologies (ISCIT),* 2012, pp.296-301.
8. H. Om, A. Kundu, "A hybrid system for reducing the false alarm rate of anomaly intrusion detection system," in *Proceedings of* *2012 1st International Conference on Recent Advances in Information Technology (RAIT),* 2012*,*  pp.131-136
9. Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, K. Dai, “An efficient intrusion detection system based on support vector machines and gradually feature removal method,” *Expert Systems with Applications*, vol. 39, n. 1, pp. 424-430, 2012.
10. S. S. S. Sindhu, S. Geetha, A. Kannan, “Decision tree based light weight intrusion detection using a wrapper approach,” *Expert Systems with Applications*, vol. 39, n. 1, pp. 129-141, 2012.
11. G. A. Carpenter, S. Grossberg & D. B Rosen, “Fuzzy ART: fast stable learning and categorization of analog patterns by an adaptive resonance system,” *Neural Networks*, vol. 4, n. 1, pp. 759-771, 1991.
12. Miroslav Kubat, Robert C. Holte, and Stan Matwin, “Machine learning for the detection of oil spills in satellite radar images,” *Machine Learning*, vol. 30, n. 2-3, pp. 195–215, 1998.
13. A. H. Fielding and J. Bell, “A review of methods for the assessment of prediction errors in conservation presence/absence models,” *Environmental Conservation*, vol. 24, n. 1, pp. 38-49, 1997.
14. J. Huang, M. Georgiopoulos and G. Heileman, “Fuzzy ART Properties,” *Neural Networks*, vol. 8, n. 2, pp. 203-213, 1995.
15. The Mathworks. "Matlab 7 Getting Started Guide", 2008.