Reaching a Consensus on Access Detection by a Decision System

César Guevara
Dep. Computer Architecture and Automatic Control
Complutense University of Madrid
Madrid, Spain
cesargue@ucm.es

Matilde Santos
Dep. Computer Architecture and Automatic Control
Complutense University of Madrid
Madrid, Spain
msantos@ucm.es

José Antonio Martín
Dep. Computer Architecture and Automatic Control
Complutense University of Madrid
Madrid, Spain
jamartinh@fdi.ucm.es

Victoria López
Dep. Computer Architecture and Automatic Control
Complutense University of Madrid
Madrid, Spain
vlopezlo@ucm.es

Abstract—**Classification techniques based on Artificial Intelligence are computational tools that have been applied to detection of intrusions (IDS) with encouraging results. They are able to solve problems related to information security in an efficient way. The intrusion detection implies the use of huge amount of information. For this reason heuristic methodologies have been proposed. In this paper, decision trees, Naive Bayes, and supervised classifying systems UCS, are combined to improve the performance of a classifier. In order to validate the system, a scenario based on real data of the NSL-KDD99 dataset is used.**

Keywords-artificial intelligence; heuristic methodologies; intrusiondDetection (IDS); decision trees; supervised dlassifying system UCS; naive Bayes

I. INTRODUCTION

Currently, Intrusion Detection Systems (IDS) are commonplace for network security and computer systems, and more and more frequently new forms of attacks, some considerably complex, appear [1].

The majority of IDS analyzes the traffic of the network and rejects whatever intrusion of a user in the information system. The analysis completed by the IDS takes places generally at a low level, generating isolated alarms and handling an immense quantity of information. Other types of IDS utilize what is called an anomalies filter that is applied to the information of the server and the databases.

The field of intrusion detection continues as an open research line concerning the developing of dynamic methodologies that are able to adapt themselves to the evolution of the computer attacks, each time more sophisticated and complicated. The strategies that IDS utilizes can be classified into two groups: detection of incorrect use, and detection of anomalies. The methodology of the Intrusion Detection Based on Anomalies, the strategy which is discussed in this article, is demanding and complex. Although it has reached good results, it is not entirely adaptable to the needs of the current technologies.

The detection of the incorrect use of a computer system requires the knowledge of the sequence of activities that constitutes an attack, which must have been stored in a database. The stored information is compared with the patterns of previous attacks. If they coincide, an alarm or warning is set off. This is the most commonly used strategy and in fact there are even commercial software that facilities it. Its main advantages lies in the speed, as it is just to find the similarity with the pattern of intrusion (already uploaded) and that the number of false positives is generally low (reliability and precision). However, some disadvantages are the incapacity to detect new attacks in a dynamic way, and furthermore the necessity of being continually updating the patterns´ databases with new cases [2, 3]. So, it is based on the intrusion behaviour and tries to identify this pattern.

On the other hand, detection of anomalies is based on the information of the normal behavior of a user. Every other different behavior is identified as an intrusion. Therefore it is based on the normal behavior pattern. Some of the disadvantages are that this method generates a considerable amount of false positives and the normal behavior of the users is quite difficult to be modeled, mainly due to the necessity of storing the information and the learning of the users´ behavior [4].

With these premises in mind, our proposal is to develop a dynamic method for the detection of intrusion by means of the analysis of the anomalies in the network traffic. The first step to reach this objective is to apply different classification strategies that come from the Artificial Intelligence field. Intrusion detection has been approached before using data mining techniques, classification in particular [5, 6].

Specifically we have tried decision trees, Naive Bayes, and supervised classification systems. Then, we combine some of

This work has been partially supported by the Ministry of Higher Education, Science, Technology and Innovation (SENESCYT) of the Government of the Republic of Ecuador.

these techniques. The main contribution of this paper is that the fusion of some classifications techniques improves the detection as it has been proved in comparison to these strategies and other when applied independently [7].

The different classification methodologies have been evaluated for the same database. The best ones have been chosen to be applied in the final classifier. As we will show, the synergy of some of them provides better results than using each technology separately. The methodology proposed should be able of processing the information in real time, filtering anomalies which could be originated by intruders. Furthermore, it should be able not only to generate alerts in the case of finding anomalies but to store them in a dynamic way to be used in the future. This way, the system learns dynamically with new cases.

The database utilized is a benchmark in the literature of security [4, 8]. Once the decision system has been proved on it, it will be applied to more complex real databases.

This article is structured as follows. The following section presents an evaluation of some classification technologies that have been analyzed. In section III a new decision making system is designed by the fusion of the ones that have provided better results. Section IV is devoted to the discussion of the results obtained by this classifier. Finally, conclusions and future work end the paper.

II. Application of Heuristic Methodologies to Intrusion Detection

In order to choose some classification techniques that allow us to design a better classifier, they have been applied to a benchmark database. We have tried some methodologies form different fields of the Artificial Intelligence discipline.

The intelligent technologies that have been applied are the following:

- Neural Networks: Multilayered Networks, Hopfield´s Neuronal Networks, Bayes Networks [9];
- Decision Trees: C4.5, ID3 [10, 11];
- Support Vector Machines (SVM) [12]
- Supervised Classifier System (UCS) [13];
- Naive Bayes (NB) [14].

In the work we have used multiple types of classification techniques that can be used to better the strong characteristics of each of these techniques. Neural networks are efficient using multiple numbers of variables. So too, the decision trees are algorithms that are efficient with a lot of information and perform the classification using all data during learning. Moreover, the "supervised classification systems" using rules based on data for the classification and its main advantage would not rule out any information. The Naive Bayes is a learning algorithm that performs continuously to obtain a better result in the classification with multiple numeric variables.

These classification techniques have been applied to the Dataset NSL-KDD[1]. It is a real database that contains information of the behavior of computer system users, both intruders and authorized ones. The NSL-KDD Dataset is made of 40 attributes or variables which provide information about the protocol, date, time, entry type, etc. In this work 25,192 registers were used for training (20% of the database NSL-KDD) and 17,102 registers for the test (13.5% of the dataset NSL-KDD), as suggested in [15].

All of the attributes included in the dataset, which describe the user´s behavior, are supposed to give relevant information and should be taken into account to improve the efficiency of a classifier based on them.

To evaluate the performance of the classification technologies, a cross validation was carried out, making use of the K-fold technique [16]. We use 10 partitions of the data (k =10) for each of the techniques. These tests gave the percentage of correctly classified cases. The accuracy of the classifier was also computed as the percentage of correctly classified users over the total number of cases for each of the eight classification techniques tested.

These previous results are shown in Figure 1. As it is possible to see, all of them present a high ratio of hits. That is because the number of examples used for the training is quite big, and therefore all the techniques give good results.

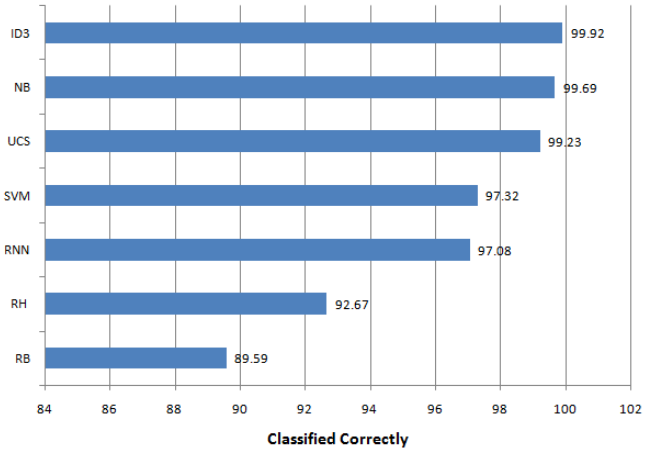

Figure 1. Percentage of correctly classified user with each technique for the dataset NSL-KDD99

More detailed information is presented in Table I. It shows different indicators of the performance of each technique, that will allow the selection of the most appropriate and efficient technique for the final decision system. In this table, the accuracy of the classification technique is also given, with the EMAE (absolute margin of error of the classifier), defined as the difference between the validity of the measurement and the validity taken exactly as an error.

Furthermore, this matrix of error shows true positives (TP) and false positives (FP) cases obtained by each technique, both

[1] NSL-KDD: http://nsl.cs.unb.ca/NSL-KDD/, 2014-03-28

for intruders and authorized user. This will help to finally make a decision on the best techniques.

TABLE I. COMPARISON OF CLASSIFICATION TECHNIQUES ON THE DATASET KSL-KDD.

Algorithm	Classified Correctly	EMAE	Accuracy	TP Genuine	TP Intruder	FP Genuine	FP Intruder
C4.5	99.96%	0.04%	0.9996	13444	11740	0	12
ID3	99.92%	0.08%	0.9992	13439	11735	1	17
NB	99.69%	0.31%	0.9969	13408	11708	32	44
UCS	99.23%	0.77%	0.9923	13346	11654	94	98
SVM	97.32%	2.68%	0.9732	13261	11258	485	188
RNN	97.08%	2.92%	0.9708	13064	11394	349	385
RH	32.67%	7.33%	0.9267	12694	10653	1090	755
RB	89.59%	10.41%	0.8959	12272	10298	1445	1177

After analyzing the performance of these techniques, four of them have been chosen for the design of the final classifier: two types of decision trees, C4.5 e ID3, Naive Bayes, and Supervised system classifier UCS as these give the best results in terms of hits.

III. FUSION OF CLASSIFICATION TECHNIQUES

A decision system for the detection of intrusions in an information system has been design based on the four classification techniques mentioned before. Figure 2 shows the classifier system that merges these methodologies.

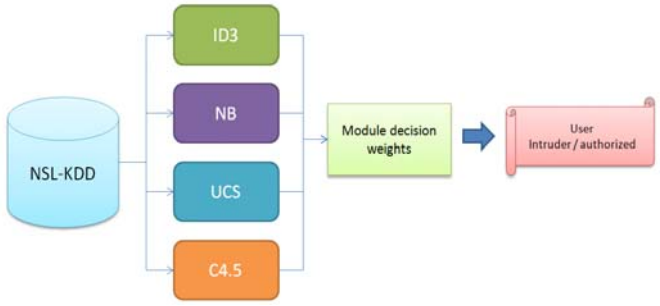

Figure 2. Fusion of Classification Techniques for the Detection of Intrusions

As it is possible to see in Figure 2, the information on the actions carried out for any user is introduced in the four classifiers. Each of them gives a result. These classifications outputs will be merged applying a rule based system.

A. *Configuration of the tools*

Each classification system has been previously trained. All of them were trained using 25,192 registers and 17,102 for the tests.

The configuration of these techniques is given below.

- **Decision Trees C4.5 and ID3:** Decision trees utilize the 40 attributes of the network´s traffic dataset and apply the algorithms J48 and ID3 for the classification.

  Before the application of the ID3 decision tree, the Iterative Dicotomizer 3 Discretizer algorithm (ID3-D)[2][8, 9], was applied to preprocessing the data of the benchmark and in order to improve its performance.

- **Naive Bayes:** The Naive Bayes technique has used all the attributes of the dataset NSL-KDD. Again a discretization algorithm, the Bayesian Discretizer (Bayesian-D) was previously used.

- **UCS:** The supervised classifier system has worked with the 40 attributes of the NSL-KDD dataset. The genetic algorithm was configured using the following values:

  - Number of explorations: 100,000;
  - Size of the initial population: 6,400 ;
  - Delta: 0.1;
  - Selection type: RWS; nu: 10.0;
  - Tournament size: 0.4;
  - Mutation type: free; probability: 0.8;
  - Cross type: 2PT; probability: 0.04;

B. *Generation of the making decision system*

The flow of the final classification system, as shown in Figure 2, is as follows.

1) **Data Input:** the network traffic information feeds the four classification systems. The 40 attributes have been previously normalized to increase the discrimination capability of each classifier [17].

2) **Classification of the inputs:** each classifier gives as result if the user is an intruder or an authorized user, with a confidence percentage.

3) **Weighting the previous results:** The results of the four previous classifiers (R1, R2, R3 and R4) are the inputs of a rule-based system.

   These results are combined according to expression (1).

$$\text{Resul} = R1 * 0.3 + R2 * 0.28 + R3 * 0.25 + R4 * 0.17 \quad (1)$$

   Different weights have been assigned to each one of the classification techniques, based on the result of Table I. The weights and techniques are as follows. C4.5 (weight = 0.3), ID3 (weight = 0.28), NB (weight = 0.25) and UCS (weight = 0.17). These values are obtained from tests with each of the techniques. The percentage is related to the number of correct detections over the total number of tests.

4) **Final decision**. A threshold is applied to the result given by expression (5). If it is greater than 0.5, it will be considered an authorized user (0); any value under 0.5 will be detected as an intruder (1).

   This value will be included in the database as a new example in order to be used in the future. So the database is dynamically increased.

[2] KEEL: http://sci2s.ugr.es/keel/index.php, 2014-03-28

IV. Results and Discussion

The indicators of the efficiency of the final making decision system are presented in Table II. The EMAE error, the accuracy of the classifier, and the true and false positives and negatives results are shown.

TABLE II. Results of the final classifier for the Detection of Intrusions.

Correctly Classified	EMAE	Accuracy	True Pos Authorized	True Pos Intruder	False Pos Authorized	False Pos Intruder
99.99%	0.1%	99.99%	10254	6835	7	6

As previously mentioned, the precision of the different classification techniques for this database was very high, due to the high number of available examples to train the methodologies. Anyway, the best ratio was 99.96 %.

With the synergy of the techniques, the new decision system has a hit ratio of 99.99%. That is, the fusion of different techniques improves the final classification ratio.

Besides, the number of false positives and false negatives values has significantly decreased. That is an interesting and useful result. Only the 0.1 % of the cases was false positives and false negatives. The information used in this study is complex and large. The classification systems were tested using different criterions, and therefore the obtained results can be considered reliable.

This study demonstrates how the fusion of different techniques may improve the results of a classification system. Once it has been proved, this synergy can be applied to more complex real problems, with uncertain or incomplete information.

V. Conclusions and Future Work

This work proposes a method for the detection of intrusions based on the fusion of four classification techniques. All of them come from the Artificial Intelligence field.

The database NSL-KDD was used as a benchmark, in order to get some knowledge of the classification process of intrusions, and to prove the validity of the proposal. The results obtained by each technique separately are worse than when merging them in a final classifier that takes all of them into account. Therefore, the detection of the intruders has improved by the synergy of different classification techniques. Not only the percentage of intrusion detection is higher but the ratio of false positives is smaller.

This is a direct benefit to the security of any computer systems. As an immediate future work, this making decision system will be applied to a real database of a governmental institution, where more variables are considered. Although the proposed method is slightly more complex than using an independent technique, we believe that when applied to more complex databases and large data, the proposal may be worth it as it is more efficient.

Acknowledgments

Authors would like to thank the reviewers for their helpful comments.

References

[1] H. Debar and J. Viinikka, "Introduction to Intrusion Detection and Security Information Management", in Foundations of Security Analysis and Design III FOSAD 2005. LNCS, 3655, pp. 207-236. Springer (2005).

[2] R.G. Bace and P. Mell. "Intrusion detection systems. Gaithersburg", in U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2001.

[3] M. Esposito , C. Mazzariello, F. Oliviero, S.P. Romano, and C. Sansone “Evaluating pattern recognition techniques in intrusion detection systems.” in Proceedings of the 5th Interna-tional Workshop on Pattern Recognition in Information Systems (PRIS) 2005, May 2005, pp. 144 - 153.

[4] W. Lee , S.J. Stolfo, and K. Mok, "Data Mining in work flow environments: Experiments in intrusion detection." in Proceedings of the 1999 Conference on Knowledge Dis-covery and Data Mining.

[5] V. Jaiganesh, S. Mangayarkarasi and P. Sumathi, "Intrusion Detection Systems: A Survey and Analysis of Classification Techniques." vol, 2, 1629-1635.

[6] A. Mitrokotsa and C. Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection.", Ad Hoc Networks, 11(1), 226-237.

[7] C. Guevara, M. Santos, and J.A. Martín-H, "Identification of Computer Information System Intruders by Decision Trees and Artificial Neural Networks" in International Conference on Intelligent Systems and Knowledge Engineering ISKE 2013.

[8] W. Wang, X. Zhang, S. Gombault, and S.J. Knapskog, "Attribute Normalization in Network Intrusion Detection", IEEE, 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks. 978-0-7695-3908-9/09, pp-448-453.

[9] S. Haykin, "Neural networks: a comprehensive foundation.", New York: Macmillan, 2004.

[10] J.R. Quinlan, "Induction of Decision Trees. Machine Learning 1", (1986) 81-106.

[11] C. X. Ling, Q. Yang, J. Wang, and S. Zhang, "Decision trees with minimal costs." in Proceedings of the twenty-first international conference on Machine learning, (2004, July), (p. 69). ACM.

[12] S. Abe, "Support vector machines for pattern classification.", London: Springer, 2005.

[13] E. Bernadó-Mansilla and J.M. Garrell., "Accuracy-Based Learning Classifier Systems: Models, Analysis and Applications to Classification Tasks." in Evolutionary Computation 11:3 (2003) 209-238.

[14] P. Domingos and M. Pazzani, "On the optimality of the simple Bayesian classifier under zero-one loss." in Machine Learning 29 (1997) 103-137.

[15] "NSL-KDD data set for network-based intrusion detection systems.” Available: http://nsl.cs.unb.ca/NSL-KDD/, March 2014.

[16] A.W. Moore and M.S. Lee, "Efficient Algorithms for Minimizing Cross Validation Error.", in Machine Learning: Proceedings of the Eleventh International Conference, Morgan Kaufmann, 1993.

[17] M. Santos , J. A. Martín H, V. López and G. Botella, "Dyna-H: A heuristic planning reinforcement learning algorithm applied to role-playing game strategy decision systems", Knowledge-Based Systems (2012), 32, 28-36.