Testing CAB-IDS through Mutations: on the Identification of Network Scans

Emilio Corchado, Álvaro Herrero, José Manuel Sáiz

Department of Civil Engineering, University of Burgos, Spain
{escorchado, ahcosio, jmsaiz}@ubu.es

Abstract. This study demonstrates the ability of powerful visualization tools (based on the use of connectionist models) to identify network intrusion attempts in an effective and reliable manner. It presents a novel technique to test and evaluate a previously developed network-based intrusion detection system (IDS). This technique applies mutant operators and is intended to test IDSs using numerical data sets. It should be made clear that some mutations were discarded as they did not all provide real life situations. As an application example of the proposed testing model, it has been specially applied to the identification of network scans and mutations of these. The tested Connectionist Agent-Based IDS (CAB-IDS) is used as a method to investigate the traffic which travels along the analysed network, detecting anomalous traffic patterns. The specific tests performed in this study were based on the mutation of one or several variables analysed by CAB-IDS.

1 Introduction

Intrusion Detection Systems (IDSs) are tools designed to monitor and analyse computer system or network events in order to detect suspect patterns that may relate to a network or system attack. An IDS that analyses packets travelling over an entire network is referred to as a network-based IDS.

Visualization techniques are starting to be applied in the field of IDSs [1], [2], [3], [4], [5], [6] and they are generally applied to numeric data. However, in the field of Computer Security, traffic data sets normally have a categorical and/or textual nature and their conversion into a data type to which visualization techniques (such as scatter plot or projectionist models) may be applied is not always obvious. Previous attempts are presented in [1], [4], [5], [6].

IDS evaluation is not a clear cut task [7]. Previous works have presented several techniques to test and evaluate misuse detection models for network-based IDSs. Some of these techniques were based [8] on a mechanism that generates a large number of variations on a known exploit by applying mutant operators to its template. In this study, a method is proposed to apply such a mutation technique for visualization techniques using numerical data sets.

In this case, the method is used to analyse the response of CAB-IDS (Connectionist Agent-Based IDS) [4], [5], [6] in the detection of a network scan. The ability to detect such scans can help to identify wider and potentially more dangerous threats to a

network. The main advantage of this testing model is that it allows analysis of IDSs based on numerical data sets.

A port scan may be defined as series of messages sent to different port numbers to gain information on its activity status. These messages can be sent by an external agent attempting to access a host to find out more about the network services this host is providing. A port scan provides information on where to probe for weaknesses, for which reason scanning generally precedes any further intrusive activity. This work focuses on the identification of network scans, in which the same port is the target for a number of computers. A network scan is one of the most common techniques used to identify services that might then be accessed without permission [3].

The principal research interest and novelty of this work lies in the development of a testing method. The main goal of this method is to prove the effectiveness and capability of any IDS based on numerical data to confront unknown attacks. In this particular study it has been used to test CAB-IDS.

2 CAB-IDS

CAB-IDS (Connectionist Agent-Based Intrusion Detection System) is a tool that has previously been described [4], [5] and can be defined as an IDS formed of different software agents [9] that work in unison [6] in order to detect anomalous situations by taking full advantage of an unsupervised connectionist model.

To detect anomalous situations, CAB-IDS consists of different kinds of agents:

- Sniffer Agent (S-A): this type of agent "controls" each segment (in which the network is divided).
- IDS Agent (IDS-A): there is only one agent of this kind, which is in charge of processing the information sent by S-As and alerting the network administrator.

The different functions performed by these agents are:

- 1st step.- Network Traffic Capture: captures packets travelling over the network segments where S-As are located.
- 2nd step.- Data Pre-processing: the captured data is selected, pre-processed and sent to the IDS-A. A set of packets and features contained in the headers of the captured data is selected from the raw network traffic.
- 3rd step.- Data Analysis: once the IDS-A receives the pre-processed data, a connectionist model (see Sect. 2.1) is applied to analyse the data and identify anomalous patterns.
- 4th step.- Visualization: the projections are presented to the network administrator.

2.1 The Unsupervised Connectionist Model

The data analysis task performed by the IDS-A is based on the use of a neural Exploratory Projection Pursuit (EPP) [10], [11] model called Cooperative Maximum Likelihood Hebbian Learning (CMLHL) [12], [13], [14]. It was initially applied in the field of Artificial Vision [12], [13] to identify local filters in space and time. In CAB-

IDS it is applied in the field of Computer Network Security. CMLHL is based on Maximum Likelihood Hebbian Learning (MLHL) [15], [16] adding lateral connections [12], [13] which have been derived from the Rectified Gaussian Distribution [17]. The resultant net can find the independent factors of a data set but does so in a way that captures some type of global ordering in the data set.

Considering an N-dimensional input vector (x), an M-dimensional output vector (y) and with W_{ij} being the weight (linking input j to output i), CMLHL can be expressed [12], [13], [14] as:

1. Feed-forward step:

$$y_i = \sum_{j=1}^{\mathbf{N}} W_{ij} x_j, \forall i \ . \tag{1}$$

2. Lateral activation passing:

$$y_i(t+1) = \left[y_i(t) + \tau(b - Ay) \right]^+ \ . \tag{2}$$

3. Feedback step:

$$e_j = x_j - \sum_{i=1}^{M} W_{ij} y_i, \forall j \ . \tag{3}$$

4. Weight change:

$$\Delta W_{ij} = \eta . y_i . sign(e_j) | e_j |^{p-1} \ . \tag{4}$$

Where: η is the learning rate, τ is the "strength" of the lateral connections, b the bias parameter, p a parameter related to the energy function [13], [15], [16] and A a symmetric matrix used to modify the response to the data. The effect of this matrix is based on the relation between the distances among the output neurons.

3 A Mutation Testing Model for Numerical Data Sets

Testing an IDS tool is the only way to establish its effectiveness. In order to test CAB-IDS, it was decided to measure its results confronting unknown anomalous situations. Furthermore, it was decided to compare it alongside other models such as Principal Component Analysis (PCA) [18] or MLHL [10], [11] as no other IDS, as far as the authors are aware, shares similar characteristics. It is noticeable that few unsupervised methods have been applied to the field of IDSs. Examples include PCA [1], EPP [4], [5] and Self-Organizing Maps (SOM) [19], [20]. Projectionist models such as PCA, EPP, MLHL or CMLHL have one important advantage over SOM in the field of computer network security in that they use time as a key variable when analysing the evolution of the packets in the traffic data set.

Misuse IDSs based on signatures rely on models of known attacks. The effectiveness of these IDSs depends on the "goodness" of their models. This is to say, if a model of an attack does not cover all the possible modifications, the performance of the IDS will be greatly impaired.

Our mutation testing model is inspired by previous testing models [8], [21], but this is the first one for IDSs based on numerical data sets. In general, a mutation can be defined as a random change. In keeping with this idea, the testing model modifies different features of the numerical information extracted from the packet headers.

The modifications created by this model may involve changes in aspects such as: attack length (amount of time that each attack lasts), packet density (number of packets per time unit), attack density (number of attacks per time unit) and time intervals between attacks. The mutations can also concern both source and destination ports, varying between the different three ranges of TCP/UDP port numbers: well known (from 0 to 1023), registered (from 1024 to 49151) and dynamic and/or private (from 49152 to 65535).

Time is another fascinating issue of great importance when considering intrusions since the chance of detecting an attack increases in relation to the duration of it. There are therefore two main strategies:

- Drastically reduce the time used to perform a scan.
- Spread the packets out over time, which is to say, reduce the number of packets sent per time unit that are likely to slip by unnoticed.

It should be taken into account and will be explained further on that any of the possible mutations may be meaningless such as a sweep of less than 5 hosts in the case of a network scan.

Several tests have been designed to verify the performance of CAB-IDS. Each test is related to a data set obtained by mutating the original one (see Sect. 4). Changes were made to the traffic related to the sweeps to take the following points into account:

- Number of sweeps in the scan (that is, number of scanned ports).
- Destination port numbers at which sweeps are aimed.
- Time intervals when sweeps are performed.
- Number of packets (density) forming the sweeps (number of scanned hosts).

Taking these issues into account, the collection of data sets designed for the research (see Sect. 4) covers the majority of the different scan-related situations with which a network might be confronted. Despite the fact that this technique is unable to provide a formal evaluation, it represents in our opinion a good approximation.

4 Data Sets and Tests

It was previously indicated that the proposed CAB-IDS [4], [5], [6] is able to identify a network scan contained in a data set with the following attributes:

- Three different sweeps to several hosts.
- Each sweep aimed at port numbers 161, 162 and 3750.
- A time difference between the first and the last packet included in each sweep of 17 866 ms for port number 161, 22 773 ms for port number 162 and 17 755 ms for port number 3750.
- An MIB (Management Information Base) information transfer event. This anomalous situation and its potential risks are fully described in [4], [5].

As previously explained, several testing data sets containing the following key features were presented to CAB-IDS following their mutation in order to measure the performance of CAB-IDS:

- Case 1 (modifying both the amount of sweeps and the destination ports):
  - Data set 1.- only one sweep: port 3750.
  - Data set 2.- two sweeps: ports 161 and 162.
  - Data set 3.- only one sweep: port 1734.
  - Data set 4.- two sweeps: ports 4427 and 4439.
- Case 2 (modifying both time and the number of sweeps):
  - Data set 5.- three time-expanded sweeps: ports 161, 162 and 3750.
  - Data set 6.- three time-contracted sweeps: ports 161, 162 and 3750.
  - Data set 7.- one time-expanded sweep: port 3750.
- Case 3 (modifying both the amount of packets and the destination ports):
  - Data set 8.- two 5-packet sweeps: ports 4427 and 4439.
  - Data set 9.- two 30-packet sweeps: ports 1434 and 65788.

The first issue to consider is the amount of sweeps in the scan. Data sets containing 1 sweep (Data sets 1, 3 and 7), 2 sweeps (Data sets 2, 4, 8 and 9) or 3 sweeps (Data sets 5 and 6) have been used. Each sweep is aimed at a different port number. The implications are crystal clear; hackers can check the vulnerability of as many services/protocols as they want. The number of sweeps (ranging from 1 to 65 536) can be modified from one scan to another.

A scan attempting to check port protocol/service can be aimed at any port number (from 0 to 65535). The data sets contain sweeps aimed at port numbers such as 161 and 162 (well known ports assigned to Simple Network Management Protocol), 1434 (registered port assigned to Microsoft-SQL-Monitor, the target of the W32.SQLExp.Worm), 3750 (registered port assigned to CBOS/IP ncapsalation), 4427 and 4439 (registered ports, as yet unassigned) and 65788 (dynamic or private port).

In order to check our system in relation to the time-related strategies, data sets 5, 6 and 7 were used. Data set 5 was obtained by spreading the packets contained in the three different sweeps (161, 162 and 3750) over the captured session. In this data set, there is a time difference of 247 360 ms between the first (in the sweep aimed at port 161) and the last scan packet (in the sweep aimed at port 3750). The duration of the captured session (all the packets contained in the data set) is 262 198 ms, whereas in the original data set the scan lasts 164 907 ms. In the case of data set 7, the same mutation has been performed but only for packets relating to the sweep aimed at port 3750. On the other hand, the strategy of reducing the time was used to obtain data set 6. In this case, the time difference between the first and the last packet is about 109 938 ms.

Finally, the number of packets contained in each sweep was also considered. In the case of a network scan, each packet means a different host included in the scan. Data sets 8 and 9 were designed with this issue in mind. Data set 8 contains low-density sweeps given that they have been reduced to only 5 packets. It was decided that a sweep scanning less than 5 hosts should not constitute a network scan. This is a fuzzy lower limit because it could also be set as 4 or 6 packets. On the other hand, data set 9 contains medium-density sweeps. In this case, each one of them has been extended to 30 packets. This is also a fuzzy upper limit.

Apart from identifying the mutated sweeps, the detection of the MIB information transfer contained in all the data sets also represented a serious test for the performance of CAB-IDS. The experimental results obtained for these data sets are shown in the following section.

5 Results and Comparison

All the results were obtained by training the connectionist model for each new data set. The application of our model to the different scenarios (see Sect. 4) led to the results that are shown in Figs.1 to 6. Only figures for the most representative cases are presented. Through these figures, it may be seen how CAB-IDS is able to identify the different mutated anomalous situations, even though some are identified with greater clarity than others. Apart from traffic related to the scan, these figures also show packets interrelated with the rest of the traffic.

Situations are labelled anomalous whenever they tend not to resemble parallel and smooth directions (normal situations). In Fig. 1 two anomalous situations are highlighted (MIB information transfer and the network scan), both identified by CMLHL. As previously explained in [4], [5], [6], those situations are identified by CMLHL as anomalous by taking account of such aspects as traffic density or "anomalous" traffic directions.

Considerable experience is required to identify the sweep in the case of the projection for data set 7 (Fig. 2). Conversely, the other anomalous situation (the MIB information transfer) is identified with far greater clarity than in any of the other cases.

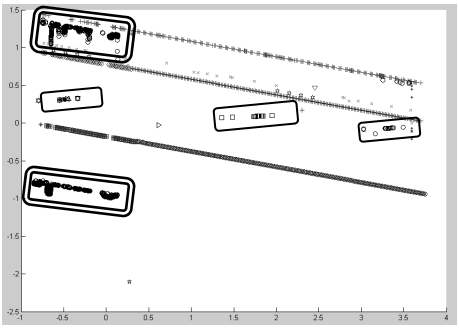

Fig. 1. CMLHL projection for data set 5

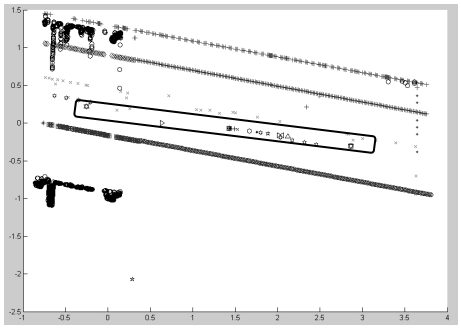

Fig. 2. CMLHL projection for data set 7

When sweeps contain only 5 packets (Data set 8 – Fig. 3), an expert is once again required to identify the anomalous scan situations. On the other hand, CAB-IDS very clearly detects high-density sweeps (Fig. 4).

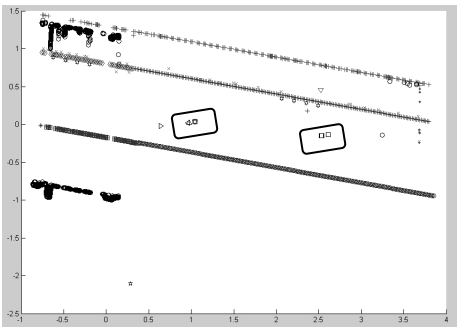

Fig. 3. CMLHL projection for data set 8

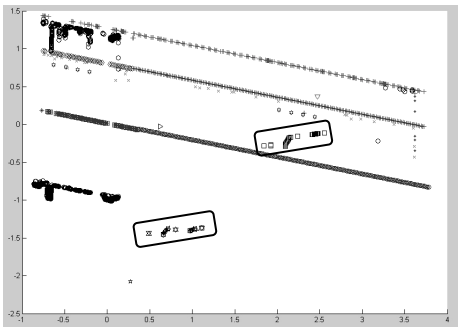

Fig. 4. CMLHL projection for data set 9

For comparison purposes, we have also applied PCA to the previous mutated data. As it can be seen in Fig. 5, the best PCA projection (Factor pair 1-3) is capable of identifying the 3-sweep scan but it is not capable of identifying the MIB information transfer. The projection of the two first principal components (Factor pair 1-2) obtained by applying PCA is unable to detect these anomalous situations. On the other hand, Fig. 6 shows how CMLHL is capable of identifying both situations.

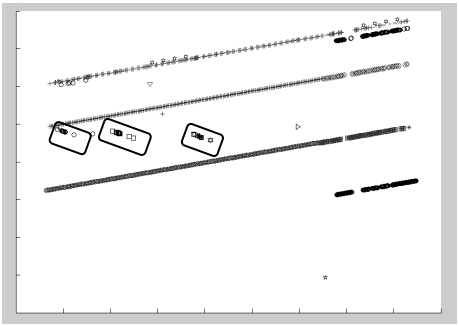

Fig. 5. PCA projection for data set 6

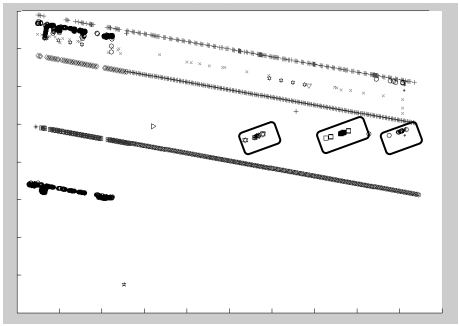

Fig. 6. CMLHL projection for data set 6

6 Conclusions and Future Work

This paper has introduced a novel mutation testing model for IDSs oriented to analyse numerical traffic data sets. It was used to test CAB-IDS and demonstrate its ability to identify most of the anomalous situations it confronted. The identification of these mutated scans can, in broad terms, be explained by the generalization capability of the connectionist model applied in this work. That is to say, through the use of one of these models, the IDS is capable of identifying not only the real anomalous situations contained in the data sets (known) but also the mutated (unknown) ones which may be real. This generalization capability of CAB-IDS represents its main advantage over the majority of signature-based IDSs. Future work will be based on the application of new learning rules to improve CMLHL.

Acknowledgments

This research has been supported by the MCyT project TIN2004-07033 and the project BU008B05 of the JCyL.

References

1. Goldring, T.: Scatter (and Other) Plots for Visualizing User Profiling Data and Network Traffic. ACM Workshop on Visualization and Data Mining for Computer Security (2004) 119–123
2. Muelder, Ch., Ma, K-L., Bartoletti: Interactive Visualization for Network and Port Scan Detection. 8th International Symposium on Recent Advances in Intrusion Detection (RAID). Lecture Notes in Computer Science, Vol. 3858. Springer-Verlag, Berlin Heidelberg New York (2005) 265–283
3. Abdullah, K., Lee, Ch., Conti, G., Copeland, J.A.: Visualizing Network Data for Intrusion Detection. IEEE Workshop on Information Assurance and Security (2002) 100–108
4. Herrero, A., Corchado, E., Sáiz, J.M.: Identification of Anomalous SNMP Situations Using a Cooperative Connectionist Exploratory Projection Pursuit Model. International Conference on Intelligent Data Engineering and Automated Learning (IDEAL). Lecture Notes in Computer Science, Vol. 3578. Springer-Verlag, Berlin Heidelberg New York (2005) 187–194
5. Corchado, E., Herrero, A., Sáiz J.M.: Detecting Compounded Anomalous SNMP Situations Using Unsupervised Pattern Recognition. International Conference on Artificial Neural Networks (ICANN). Lecture Notes in Computer Science, Vol. 3697. Springer-Verlag, Berlin Heidelberg New York (2005) 905–910
6. Corchado, E., Herrero, A., Sáiz, J.M.: A Feature Selection Agent-Based IDS. First European Symposium on Nature-Inspired Smart Information Systems (2005)
7. Ranum, M.J.: Experiences Benchmarking Intrusion Detection Systems. NFR Security (2001)
8. Vigna, G., Robertson, W., Balzarotti, D.: Testing Network-Based Intrusion Detection Signatures Using Mutant Exploits. ACM Conference on Computer and Communication Security (ACM CCS) (2004) 21–30
9. Wooldridge, M.: Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence, Gerhard Weiss (1999)
10. Friedman J., Tukey. J.: A Projection Pursuit Algorithm for Exploratory Data Analysis. IEEE Transaction on Computers, Vol. 23 (1974) 881-890
11. Hyvärinen A.: Complexity Pursuit: Separating Interesting Components from Time Series. Neural Computation, Vol. 13(4) (2001) 883-898
12. Corchado, E., Han, Y., Fyfe, C.: Structuring Global Responses of Local Filters Using Lateral Connections. Journal of Experimental and Theoretical Artificial Intelligence, Vol. 15(4) (2003) 473–487
13. Corchado, E., Fyfe, C.: Connectionist Techniques for the Identification and Suppression of Interfering Underlying Factors. International Journal of Pattern Recognition and Artificial Intelligence, Vol. 17(8) (2003) 1447–1466
14. Corchado, E., Corchado, J.M., Sáiz, L., Lara, A.: Constructing a Global and Integral Model of Business Management Using a CBR System. First International Conference on Cooperative Design, Visualization and Engineering (CDVE). Lecture Notes in Computer Science, Vol. 3190. Springer-Verlag, Berlin Heidelberg New York (2004) 141–147
15. Corchado, E., MacDonald, D., Fyfe, C.: Maximum and Minimum Likelihood Hebbian Learning for Exploratory Projection Pursuit. Data Mining and Knowledge Discovery, Vol. 8(3), Kluwer Academic Publishing (2004) 203–225
16. Fyfe, C., Corchado, E.: Maximum Likelihood Hebbian Rules. European Symposium on Artificial Neural Networks (2002) 143–148
17. Seung, H.S., Socci, N.D., Lee, D.: The Rectified Gaussian Distribution. Advances in Neural Information Processing Systems, Vol. 10 (1998) 350–356
18. Oja, E.: Neural Networks, Principal Components and Subspaces. International Journal of Neural Systems, Vol. 1 (1989) 61–68
19. Hätönen, K., Höglund, A., Sorvari, A.: A Computer Host-Based User Anomaly Detection System Using the Self-Organizing Map. International Joint Conference of Neural Networks (2000) 411–416
20. Zanero, S., Savaresi, S.M.: Unsupervised Learning Techniques for an Intrusion Detection System. ACM Symposium on Applied Computing (2004) 412-419
21. Marty, R.: Thor: A Tool to Test Intrusion Detection Systems by Variations of Attacks. ETH Zurich. Diploma Thesis (2002)