A cooperative connectionist IDS model to identify independent anomalous SNMP situations

Álvaro Herrero, Emilio Corchado, José Manuel Sáiz
Department of Civil Engineering, University of Burgos, Spain
escorchado@ubu.es

Abstract

This research approaches the anomalous situations detection issue from a pattern recognition point of view, where a connectionist model is applied to identify user behavior patterns. The aim of this multidisciplinary research is the design of a system capable of detecting anomalous situations for a computer network. The connectionist architecture used here has never been applied to the Intrusion Detection (ID) and network security fields before this research. This work line demonstrates that connectionist models are capable of satisfying the requirements and dynamic features of the ID problem. By exploiting the strengths of neural networks in recognition, classification and generalization, this work illustrates the effectiveness of these techniques to the ID field. The presented Intrusion Detection System (IDS) is used as a method to investigate the traffic that travels along the analysed network, detecting SNMP (Simple Network Management Protocol) anomalous traffic patterns. It is also shown how the system is capable of detecting independent SNMP anomalous situations. It helps network administrators to decide if these anomalous situations are real intrusions or not.

1. Introduction

IDS are hardware or software systems that monitor the events occurring in a computer system or network, analysing them to identify computer security problems. They have become a necessary additional tool to the security infrastructure as the number of network attacks has increased very fast during the last years.

Currently there are several techniques to implement IDS. Some of them are based on the use of expert systems (containing a set of rules that describe attacks), signature verification (where attack scenarios are converted into sequences of audit events), petri nets (where known attacks are presented with graphical petri nets) or state-transition diagrams (representing attacks with a set of goals and transitions). One of the main disadvantages of these techniques is the fact that new attack situations are not automatically discovered without updating the IDS.

Connectionist models have been identified as a very promising technique of addressing the ID problem due to two main features: they are suitable to detect day-0 (previously unknown) attacks and they have the ability to classify patterns (attack classification, alert validation). Up to now, there have been several attemps to apply artificial neural architectures (such as Self-Organising Maps [15, 22] or Elman Networks [14]) to the network security field [6, 7, 9]. This paper presents an IDS based on a neural architecture which has never been applied to the ID problem before.

In the short-term, the Simple Network Management Protocol (SNMP) can be defined as a protocol oriented to manage nodes in the Internet community [1]. This is, it is used to control routers, bridges, and other network elements, reading and writing a wide variety of information about the device: operating system, routing tables, default TTL (Time To Live), and so on. Some of this data can be extremely sensitive [18]. We have decided to study SNMP anomalous situations because an attack based on this protocol may severely compromise the systems security. CISCO [2] found the top five

Actas del III Taller Nacional de Minería de Datos y Aprendizaje, TAMIDA2005, pp.179-184
ISBN: 84-9732-449-8 © 2005 Los autores, Thomson

most vulnerable services in order of importance, and SNMP was one of them.

All the traffic travelling along the network has been taken into account to ensure the existence of both, anomalous and non-anomalous situations.

2. The unsupervised pattern recognition model

The Data Classification and Result Display steps (Figure 1) performed by this IDS model are based on the use of a neural EPP model called Cooperative Maximum Likelihood Hebbian Learning (CMLHL) [3, 4, 5].

Exploratory Projection Pursuit (EPP) [8, 10, 13, 16] is a statistical method for solving the difficult problem of identifying structure in high dimensional data. It is based on the projection of the data onto a lower dimensional subspace in which we search for its structure by eye. It is necessary to define an “index” that measures the interestingness of a projection. After that, the data is transformed by maximizing the index in order to maximize the interest according to that index. From a statistical point of view the most interesting directions are those that are as non-Gaussian as possible.

Cooperative Maximum Likelihood Hebbian Learning (CMLHL) was initially applied to the field of Artificial Vision [4, 5] to identify local filters in space and time. Here, we have applied it to the computer security field [6, 7]. It is based on Maximum Likelihood Hebbian Learning (MLHL) [8, 13]. Consider an N-dimensional input vector, $\mathbf{x}$, and an M-dimensional output vector, $\mathbf{y}$, with W_{ij} being the weight linking input (j) to output (i) and let η be the learning rate.

CMLHL can be expressed as:

- Feed forward:

$$y_i = \sum_{j=1}^{\mathbf{N}} W_{ij} x_j, \forall i \qquad (1)$$

- Lateral activation passing:

$$y_i(t+1) = [y_i(t) + \tau(b - Ay)]^+ \qquad (2)$$

- Feedback:

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

- Weight change:

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

Lateral connections [4, 5] have been derived from the Rectified Gaussian Distribution [21] and applied to MLHL. The resultant net can find the independent factors of a data set but do so in a way that captures some type of global ordering in the data set.

3. Connectionist IDS model

The information analysed by our system is obtained from the packets that travel along the network. So, it is a Network-Based IDS. The necessary data for the traffic analysis is contained on the captured packets headers and it can be obtained using a network analyser.

The structure of this novel IDS model is shown in Figure 1 and it is described as follows:

- *1st step.- Network Traffic Capture*: one of the network interfaces is set up as “promiscuous” mode. It captures all the packets travelling along the network.
- *2nd step.- Data Pre-processing*: the captured data is pre-processed and introduced as the input data to the following stage.
- *3rd step.- Data Classification*: once the data has been pre-processed, the pattern recognition model (section 2) analyses the data and identifies anomalous patterns.
- *4th step.- Result Display*: the last step is related to the visualization stage. Finally the output is presented to the network administrator or the person in charge of the network security.

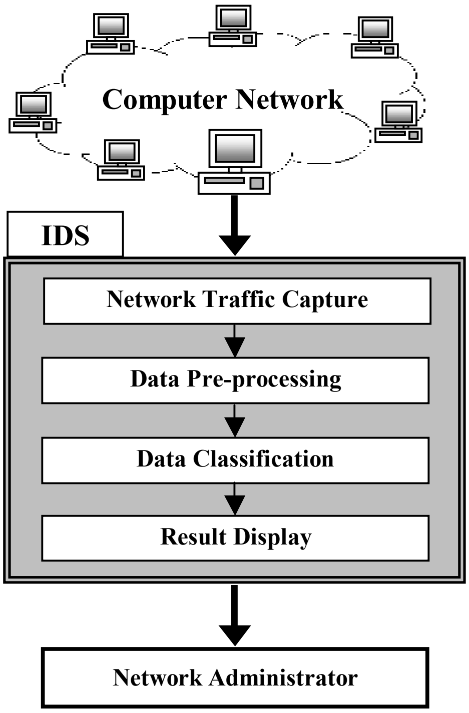

Figure 1. Structure of the Neural IDS Model

4. Independent SNMP anomalous situations in real data sets

The study of SNMP is the reason why the system selects packets based on UDP (User Datagram Protocol) during the data pre-processing layer. We only select traffic based on UDP. This means that in terms of TCP/IP (Transmission Control Protocol/Internet Protocol) protocol stack, the model analyses only the packets that use UDP at transport layer and IP at network layer.

We have focused our effort in the study of two of the most dangerous independent anomalous situations related to SNMP [6, 7]. These situations are MIB (Management Information Base) information transfer and SNMP port sweep. We have called these situations as independent ones because a "complete" attack should be formed by instances of them, making a compounded anomalous situation.

4.1. MIB information transfer

The IAB (Internet Activities Board) recommended that all IP and TCP implementations were network manageable [20]. The implementation of the Internet MIB and at least one of the management protocols like SNMP are the consequences of this suggestion.

The MIB can be roughly defined as a database that contains information about some elements or devices that can be network-controlled. This is the database used by SNMP to store information about the elements that it controls.

A MIB information transfer is a transfer of some information contained in the SNMP MIB. This is considered a quite dangerous situation because a person having some free tools, some basic SNMP knowledge and the community password (in SNMP v. 1 and SNMP v. 2) can come up with all sorts of interesting and sometimes useful information.

4.2. SNMP port sweep

This situation is a scanning of network computers for the SNMP port using sniffing methods. The aim is to make a systematic sweep in a group of hosts to verify if SNMP is active in one of the following ports: 161, 162 and 3750. The sweep has been done using these port numbers because:

- 161 and 162 are the default port numbers for SNMP, as RFC 1157 [1] says: "protocol entity receives messages at UDP port 161, and messages which report traps should be received on UDP port 162".
- We have also included a random port (3750) in the sweep as a test random element.

4.3. Characteristics of the data sets

In this work, different data sets (containing examples of the anomalous situations described above) have been analysed by the IDS:

Some features of the analysed traffic that travels along the network are the following:

- In addition to the SNMP packets, the data sets contain traffic related to other protocols installed in our network, like NETBIOS and BOOTPS.

- The SNMP packets are generated and sent inside the own network, this is, it is an internal protocol and any host out of the network cannot introduce any packets of this type in the network. This is mainly warranted by the external security implemented through the firewall.

In the Data Pre-processing step, the system performs a data selection of all the information captured. So all the data sets contain the following 5 variables extracted from the packet headers:

- *Timestamp*: the time when the packet was sent (difference in relation to the first captured packet).
- *Protocol*: all the protocols contained in the data set have been codified.
- *Source Port*: the port number of the source host that sent the packet.
- *Destination Port*: the port number of the destination host where the packet is sent.
- *Size*: total packet size (in Bytes).

5. Experimental results

The following figures (Figure 2 and Figure 3) show the best results obtained by the developed IDS, in order to analyse the data sets described before.

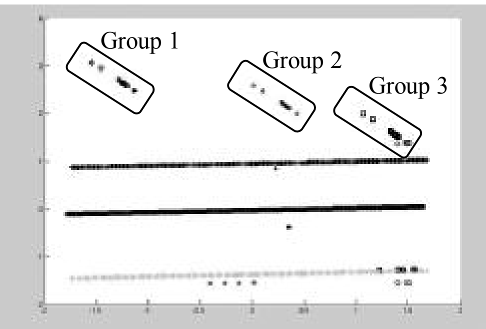

Figure 2. Best projection displayed by the model for the SNMP-port-sweep data set.

Through a simple visual analysis of Figure 2, it can be seen that while most of the traffic evolves in the same direction, it is easy to identify three groups (Groups 1, 2 and 3.- Figure 2) progressing in a different direction. Each one of these groups contains packets sent to each port included in the sweep (161, 162 and 3750), which is embedded in the data set introduced to the model. These graphical features allow the identification of the sweep anomalous situation just by looking.

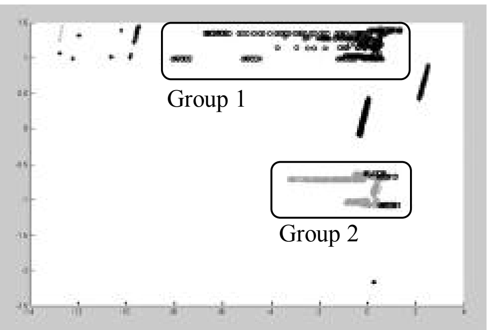

Figure 3. Best projection displayed by the model for the MIB-information-transfer data set.

In Figure 3 it is easy to identify several packet groups. Two of them (Groups 1 and 2.- Figure 3) are different than other groups (related to normal traffic). These groups are related to the SNMP transfer mentioned above: they contain packets sent and received during the transfer embedded in the data set. Group 1 (Figure 3) contains all the traffic in one way (from destination to source), while Group 2 (Figure 3) contains all the traffic in the other way (from source to destination). These groups have been labeled as anomalous ones due to two combined issues: high temporal concentration of packets, and because they are made up of different size packets, situation which is related to the MIB information transfer.

As can be seen in Figure 2 and Figure 3, the developed IDS is capable of identifying and highlighting both anomalous situations. It shows how the system works successfully in the cases where there is an anomalous situation among normal ones. In Figure 2 we have identified the sweep (Groups 1, 2 and 3) by means of normal/abnormal growth direction (in terms or parallelism) and in Figure 3 we have identified the MIB transfer (Groups 1 and 2) by means of high temporal concentration of packets.

All the packets belonging to SNMP are contained in one of these “special” groups and there are no packets belonging to another protocol.

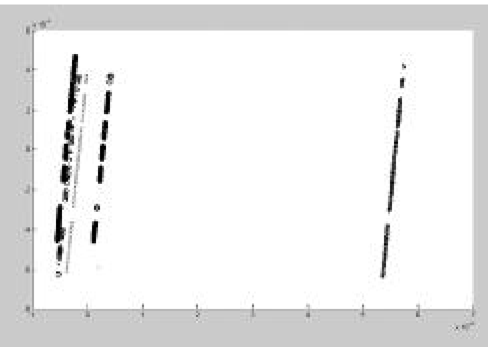

Figure 4. PCA projection for the MIB-information-transfer data set.

We have applied different connectionist methods such as Principal Component Analysis (PCA) [12, 19] to the same data sets. As it is shown before, CMLHL is capable of identifying both anomalous situations while PCA is just identifying the sweep, not detecting the MIB transfer (Figure 4).

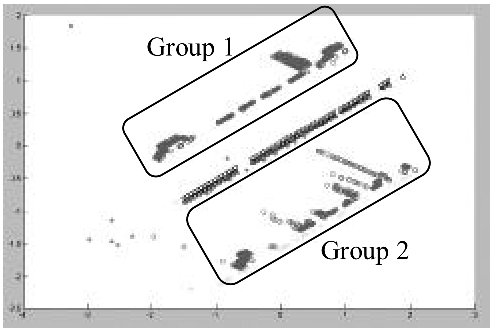

Figure 5. Best MLHL projection for the MIB-information-transfer data set.

We have also applied a more complex than PCA connectionist method: Maximum Likelihood Hebbian Learning. In this case, the differences with CMLHL are not as clear as in the case of PCA. MLHL is capable of detecting both anomalous situations, but not as clearly as CMLH do, as can be seen for the MIB information transfer data set in Figure 5. In this figure, It can be seen how MLHL detect the MIB information transfer (Groups 1 and 2 .- Figure 5) , but in a less clear way than CMLHL (Figure 3). We can resume that CMLHL provides more sparse projections [4].

6. Conclusions and future work

This research demonstrates the effectiveness and robustness of this novel IDS due to its capability to identify independent anomalous situations, showing its capacity for generalization.

In terms of performance results, we can say this model works because it has identified and distinguished both the MIB transfer and the port sweep situations (anomalous situations that we know in advance as we have chosen the toy data set).

The visualization tool used in the Result Display step, shows data projections highlighting anomalous situations clearly enough to alert the network administrator, taking into account aspects as the traffic density or “abnormal” directions. Finally, only the person in charge of the network security has the authority to decide if the anomalous situations are real intrusions or not.

Further work will be focused on the application of GRID computation [11, 17] with more complex data sets, trying to extend the model to cover several different situations, including other protocols apart from SNMP.

Acknowledgments

This research has been supported by the McyT projects: TIN2004-07033.

References

[1] Case, J., Fedor, M.S., Schoffstall, M.L., Davin, C. Simple Network Management Protocol (SNMP). RFC-1157, 1990.

[2] Cisco Secure Consulting, Vulnerability Statistics Report, 2000.

[3] 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, 2004.

[4] Corchado, E., Fyfe, C. Connectionist Techniques for the Identification and Suppression of Interfering Underlying Factors. International Journal of Pattern Recognition and Artificial Intelligence 17 (8): 1447-1466, 2003.

[5] Corchado, E., Han, Y., Fyfe, C. Structuring Global Responses of Local Filters using Lateral Connections. Journal of Experimental and Theoretical Artificial Intelligence 15 (4): 473-487, 2003.

[6] Corchado, E., Herrero, A., Baruque, B., Saiz, J.M. Intrusion Detection System Based on a Cooperative Topology Preserving Method. International Conference on Adaptive and Natural Computing Algorithms. Springer Computer Science. SpringerWienNewYork, 2005.

[7] Corchado, E., Herrero, A., Saiz, J.M. An Unsupervised Cooperative Pattern Recognition Model to Identify Anomalous Massive SNMP Data Sending. In Proceedings of the 1st International Conference on Natural Computation. ("In press") 2005.

[8] Corchado, E., MacDonald, D., Fyfe, C. Maximum and Minimum Likelihood Hebbian Learning for Exploratory Projection Pursuit. Data Mining and Knowledge Discovery. Kluwer Academic Publishing 8(3): 203-225, 2004.

[9] Debar, H., Becker, M., Siboni, D. A Neural Network Component for an Intrusion Detection System. IEEE Symposium on Research in Computer Security and Privacy, 1992.

[10] Friedman, J., Tukey, J. A Projection Pursuit Algorithm for Exploratory Data Analysis. IEEE Transaction on Computers 23: 881-890, 1974.

[11] Foster, I., Kesselman, C. The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann Publishers, 1998.

[12] Fyfe, C. A Neural Network for PCA and Beyond. Neural Processing Letters 6, 1996.

[13] Fyfe, C., Corchado, E. Maximum Likelihood Hebbian Rules. European Symposium on Artificial Neural Networks, 2002.

[14] Ghosh, A., Schwartzbard, A., Schatz, A. Learning Program Behavior Profiles for Intrusion Detection. Workshop on Intrusion Detection and Network Monitoring, 1999.

[15] 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.

[16] Hyvärinen, A. Complexity Pursuit: Separating Interesting Components from Time Series. Neural Computation 13: 883-898, 2001.

[17] Kenny, S. Towards a Grid-wide Intrusion Detection System. European Grid Conference. LNCS. SpringerWienNewYork, 2005.

[18] Myerson, J.M. Identifying Enterprise Network Vulnerabilities. International Journal of Network Management 12, 2002.

[19] Oja, E. Neural Networks, Principal Components and Subspaces. International Journal of Neural Systems 1: 61-68, 1989.

[20] Postel, J. IAB Official Protocol Standards. RFC-1100, 1989.

[21] Seung, H.S., Socci, N.D., Lee, D. The Rectified Gaussian Distribution. Advances in Neural Information Processing Systems 10: 350-356, 1998.

[22] Zanero, S., Savaresi, S.M. Unsupervised Learning Techniques for an Intrusion Detection System. ACM Symposium on Applied Computing: 412-419, 2004.