A FEATURE SELECTION AGENT-BASED IDS

Emilio Corchado, Álvaro Herrero and José Manuel Sáiz
Department of Civil Engineering, University of Burgos
C/Francisco de Vitoria s/n., 09006, Burgos, Spain
Phone: +34 947259395, email: escorchado@ubu.es

ABSTRACT: This paper introduces an Intrusion Detection System (IDS) based on the use of several Artificial Intelligence (AI) techniques. The anomalous detection issue is approached from a feature selection point of view, where a connectionist model is applied as a data analysis technique in an IDS. By exploiting the strengths of connectionist architectures in recognition, classification and generalization, this work shows the benefits of applying connectionist models and agent technology to the Intrusion Detection (ID) field. This work is based on the fact that projectionist systems have never been applied to the IDS field and network security until this research project. It helps network administrators to decide if anomalous situations are real intrusions or not. To cover the more complex situations related to segment-divided networks, we introduce a new approach based on a distributed architecture where different software agents cooperate to detect anomalous SNMP (Simple Network Management Protocol) situations in a big-size network.

KEYWORDS: connectionist models, unsupervised learning, intrusion detection systems, multi-agent systems

INTRODUCTION

Computer security actions are aimed to prevent and detect unauthorized use of computers or computer networks. IDS have become one of the most important security tool. They are hardware or software systems that monitor the events occurring in a computer system or network, analysing them to identify 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.

IDS have been previously built by hand. AI techniques can decrease the effort needed to build IDS and can also improve their performance. Some techniques are used to implement IDS (such as state-transition diagrams, expert systems, petri nets, signature verification, etc.). Among them, connectionist models have been identified as a very promising method of addressing the ID problem due to two main features: they are suitable to detect day-0 attacks and they have the ability to classify patterns (attack classification, alert validation, etc.). Up to now, there have been several attends to apply connectionist models [1] (such as Self-Organising Maps [2], [3] or Elman Networks [4]) to the network security field. This paper presents an IDS based on a connectionist architecture which has never been applied to the ID problem before this research. This architecture is called Cooperative Maximum Likelihood Hebbian Learning (CMLHL), and has been shown [5], [6], [7], [8] a very effective one to perform the data analysis process (see Figure 1).

The actual demands of effectiveness and complexity have caused the development of new computing paradigms. One of these new paradigms are agent and multi-agent systems. A software agent can be defined as a system with capacity of adaptation and provided with mechanisms allowing it to decide what to do (according to their objectives) [9]. This kind of systems has been previously used in the field of IDS [10], [11].

PROBLEM OVERVIEW

A protocol in a computer network context is a specification that describes low-level details of host-to-host interfaces or high-level exchanges between application programs. Among all the implemented network protocols we have focused our effort in the study of SNMP because an attack based on this protocol may severely compromise the system security. SNMP was identified as one of the top five most vulnerable services (in order of importance) by CISCO [12].

In the short-term, SNMP was oriented to manage nodes in the Internet community [13]. That is, it is used to control routers, bridges, and other network elements, reading and writing a wide variety of information about the devices: operating system, version, routing tables, default TTL (Time To Live) and so on. Some of this data can be extremely sensitive.

The IAB (Internet Activities Board) recommended that all IP (Internet Protocol) and TCP (Transmission Control Protocol) implementations were network manageable [14]. The implementation of the Internet Management Information Base (MIB) and at least one of the management protocols like SNMP is the consequence 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 database is used by SNMP to store information about the elements that it controls.

There are some dangerous anomalous situations related to SNMP [8], such as port sweep and MIB information transfer.

SEGMENTED SNMP (AGENT APPROACH)

An SNMP Agent is the operational role assumed by an SNMP party (generally a device controlled by this protocol) when it performs SNMP management operations in response to received SNMP messages [16]. An SNMP Proxy Agent is an SNMP Agent that performs management operations by communicating with another logically remote party. In the case of a segmented network, "logically remote" means that each party is located in a different network segment.

The transparency principle [16] defines the behavior of an SNMP party and says that the manner in which one SNMP party processes SNMP protocol messages received from another SNMP party is entirely transparent to the latter. Implicit in this principle is the requirement that, throughout its interaction with a Proxy Agent, a management station is supplied with no information about the nature or progress of the proxy mechanisms by which its requests are realized. That is, it should seem to the management station as if it were interacting via SNMP directly with the proxied device.

THE MULTI-AGENT IDS MODEL

To upgrade the connectionist IDS model previously developed [8], it is split out into different software agents [9] working together in order to detect the intrusive actions defined above.

Corporative networks can be very big-size ones, where computers are set up into different network segments, mainly caused by the IP address limitations. Here is where a distributed IDS can take advantage. By using this kind of IDS (where a "listener" entity capture the traffic travelling along each different network segment), the model is able to identify all the anomalies caused in a segment-divided network. Otherwise, only the anomalies caused in the segment where the IDS is located could be identified. All the different SNMP anomalous situations can be produced in every different segment (where SNMP Agents are set up). In order to detect all these situations we propose this distributed agent-based IDS. It is shown in Figure 1 and consists on two different kinds of agents:

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

This structure allows the system to use the source and destination IP address in such a way that every Agent could know from which network segment the packet is coming.

Sniffer Agents carry out two main functions:

- Network Traffic Capture Function: one of the network interfaces of the host where the Sniffer Agent is located is set up as "promiscuous" mode. It captures all the packets travelling along this network segment.
- Data Pre-processing Function: the captured data is selected, pre-processed and sent to the IDS Agent.

The information analysed by these Agents is obtained from the packets that travel along the network. The necessary data for the traffic analysis is contained on the captured packets headers. This data can be obtained using a network analyser. The study of SNMP is the reason why only packets based on UDP (User Datagram Protocol) are selected. This means that in terms of TCP/IP (Transmission Control Protocol/Internet Protocol) protocol stack, the model captures only the packets using UDP at transport layer and IP at network layer. So in addition to the SNMP packets, the data sets contain traffic related to other protocols installed in our network, like NETBIOS and BOOTPS.

During the Data Pre-processing Function (Figure 1), a data selection of all the information captured is performed. So the variables used are: timestamp, protocol ID, source port, destination port, source IP address, destination IP address and packet size. Only the pre-processed data is sent to the IDS Agent.

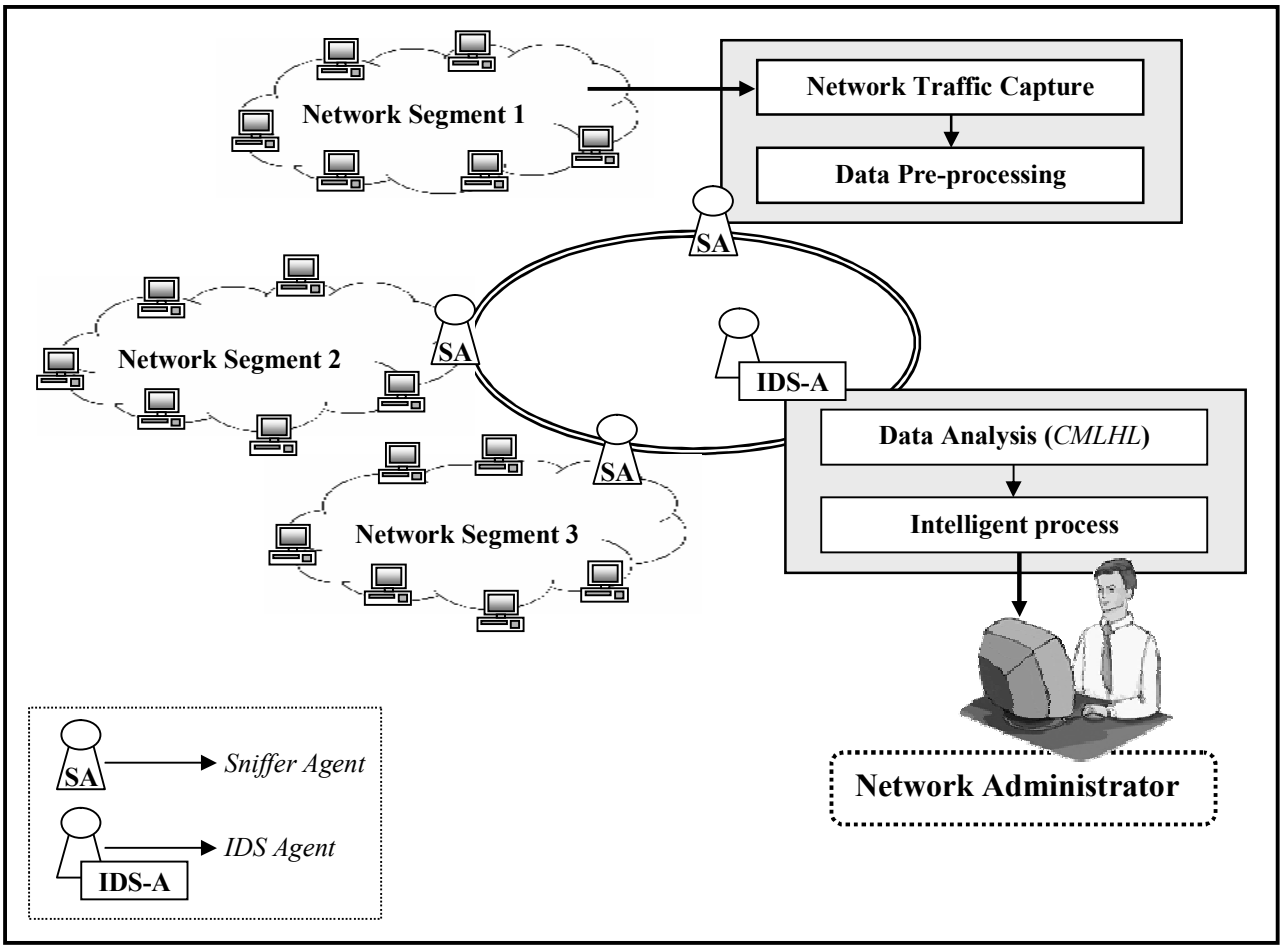

Figure 1: Structure of the Agent-Based IDS

Once the pre-processed data is received in the IDS Agent, a connectionist model (see Equations 1 to 5) is applied to analyse the data and identify anomalous patterns. With this distributed structure, this Agent is capable of identifying anomalous situations concerning to different network segments. That is, an anomalous situation can affect SNMP Agents located in different segments.

The IDS Agent can be equipped with different mechanisms to abort an attack. That is, after identifying an anomalous situation, it can carry out concrete actions to abort the attack (such as deactivating SNMP). Finally, the network administrator is alerted about the anomalous situations that are happening (or had happened) along all the segments in which the network is divided.

THE UNSUPERVISED CONNECTIONIST IDS MODEL

Exploratory Projection Pursuit (EPP) [17], [18], [19], [20] is a statistical method for solving the complex problem of identifying structure in high dimensional data. It is based on the projection of the data onto a lower dimensional subspace in which its structure is searched by eye. It is necessary to define an "index" to measure the varying degrees of interest generated by each projection. Subsequently, the data is transformed by maximizing the index and the associated interest. From a statistical point of view the most interesting directions are those that are as non-Gaussian as possible.

The Data Analysis step performed by the IDS Agent (Figure 1) is based on the use of a neural EPP model called Cooperative Maximum Likelihood Hebbian Learning (CMLHL) [21], [22], [23]. It was initially applied to the field of Artificial Vision [21], [22] to identify local filters in space and time. Here, we have applied it to the field of Computer Security. It is based on Maximum Likelihood Hebbian Learning (MLHL) [19], [20] adding lateral connections [21], [22], which have been derived from the Rectified Gaussian Distribution [24]. 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.

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:

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

Lateral connections are applied:

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

A is a symmetric matrix used to modify the response to the data whose effect is based on the relation between the distances among the output neurons. It is based on the Cooperative Distribution [24], but to speed learning up, it can be simplified to [25]:

$$A(i,j) = \delta_{ij} - \cos\left(2\pi(i-j)/M\right) \tag{3}$$

The activation (e_j) is fed back through the same weights and subtracted from the input:

$$e_j = x_j - \sum_{i=1}^{M} W_{ij} y_i, \forall j \tag{4}$$

Weight update:

$$\Delta W_{ij} = \eta . y_i . sign\left(e_j\right) | e_j |^{p-1} \tag{5}$$

Where: η is the learning rate, τ is the "strength" of the lateral connections, b is the bias parameter and p is a parameter related to the energy function [19], [20], and δ_{ij} is the Kronecker delta.

COMPARISON WITH OTHER TECHNIQUES

The projection method called MLHL, and others based on it (such as CMLHL), can show the evolution through the time of the system response. In the IDS field, the time variable (or temporal relationship between packets) is very important because it is decisive in the detection of some kinds of attacks. A high concentration in time can imply an anomalous situation by itself. A typical example of this can be a MIB information transfer, where a high temporal concentration means a transference of great quantity of information. It is a transfer of some information contained in the SNMP MIB, and is considered a quite dangerous situation because a hacker can come up with all sorts of interesting and sometimes useful information.

This variable from the dataset does not provide as much information when other unsupervised connectionist models are applied. That is the case of Self-Organising Maps (SOM) [26]. Several authors have applied this model [2], [3] in the data-analysis process without taking into account the time dimension of the data set.

On the other hand, most of the signature-verification models do not take into account this time dimension. They work at a packet level, so they cannot use the time issues of the dataset as a whole. It implies that these models do not take into account the time concentration of anomalous or risky packets, as it is done by the model proposed in this paper.

Finally, the model introduced in this work uses this important variable, allowing a dynamic analysis and a better study of the information, as can be seen in Figure 2.

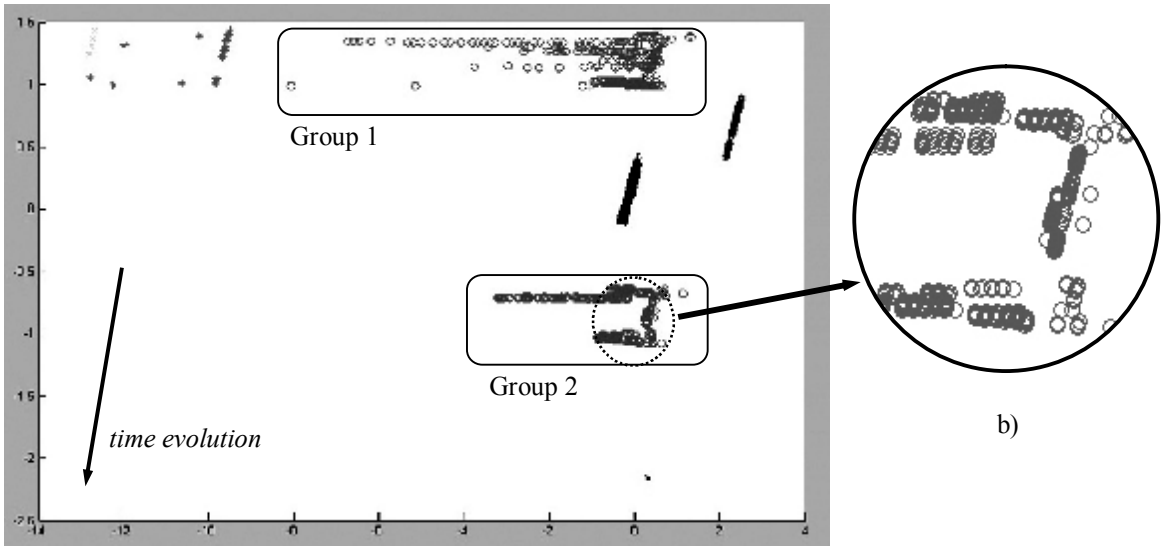

Figure 2: a) Data projection displayed by the connectionist model for a MIB information transfer.
b) Visualization of an example of a high temporal concentration of packets.

In Figure 2.a it is easy to identify several packet groups. Groups 1 and 2 are related to a MIB information transfer: they contain packets sent and received during the transfer embedded in the data set. Group 1 contains all the traffic in one way (from destination to source), while Group 2 contains all the traffic in the other way (from source to destination). These groups have been labelled 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. Figure 2.b shows a very high temporal concentration of packets, which caused the identification of Groups 1 and 2 as anomalous ones.

CONCLUSIONS

We propose an Agent-Based IDS model made up of two different kinds of agents: Sniffer Agents and IDS Agent. This model allows us to identify the attacks happening in each segment and the most general ones (those implying more than only one network segment). Automatic mechanisms can be developed and run to abort an attack.

To handle and classify all the pre-processed information related with the whole network, the IDS Agent should have a very big calculus power. The IDS Agent can be located in the most powerful machine in the organization. It does not matter what network segment this machine is located in.

ACKNOWLEDGMENTS

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

REFERENCES

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

[2] Hätönen, K.; Höglund, A.; Sorvari, A., 2000, “A Computer Host-Based User Anomaly Detection System Using the Self-Organizing Map”, International Joint Conference of Neural Networks.

[3] Zanero S.; Savaresi S.M., 2004, “Unsupervised Learning Techniques for an Intrusion Detection System”, ACM Symposium on Applied Computing, pp. 412 – 419.

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

[5] Corchado, E.; Herrero, A.; Baruque, B.; Sáiz J.M., 2005, "Intrusion Detection System Based on a Cooperative Topology Preserving Method", International Conference on Adaptive and Natural Computing Algorithms, Springer Computer Science, pp. 329 – 335.

[6] Herrero, A.; Corchado, E.; Sáiz, J.M., 2005, "Identification of Anomalous SNMP Situations Using a Cooperative Connectionist Exploratory Projection Pursuit Model", International Conference on Intelligent Data Engineering and Automated Learning, Springer-Verlag, Lecture Notes in Computer Science, vol. 3578, pp. 187 – 194.

[7] Herrero, A.; Corchado, E.; Sáiz, J.M., 2005, "A Cooperative Unsupervised Connectionist Model Applied to Identify Anomalous Massive SNMP Data Sending", International Conference on Natural Computation, Springer-Verlag, Lecture Notes in Computer Science vol. 3610, pp. 778 – 782.

[8] Corchado, E.; Herrero, A.; Sáiz J.M., 2005, "Detecting Compounded Anomalous SNMP Situations Using Unsupervised Pattern Recognition", International Conference on Artificial Neural Networks (ICANN 05), Springer-Verlag, Lecture Notes in Computer Science, vol. 3697. ("In press")

[9] Wooldridge, M., 1999, "Multiagent Systems: A Modern Approach to Distributed Artificial Inteligence", Gerhard Weiss.

[10] Spafford, E.H.; Zamboni, D., 2000, "Intrusion Detection Using Autonomous Agents", Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 34(4), pp. 547 – 570.

[11] Hegazy, I.M.; Al-Arif, T.; Fayed, Z.T.; Faheem, H.M., 2003, "A Framework for Multiagent-based System for Intrusion Detection", Intelligent Systems Design and Applications, Springer-Verlag, Adv. in Soft Computing Serie.

[12] Cisco Secure Consulting, 2000, "Vulnerability Statistics Report".

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

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

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

[16] Davin, J.; Galvin, J.; McCloghrie, K., 1992, "SNMP Administrative Model", RFC-1351.

[17] Friedman J.; Tukey. J., 1974, "A Projection Pursuit Algorithm for Exploratory Data Analysis", IEEE Transaction on Computers, vol. 23, pp. 881 – 890.

[18] Hyvärinen, A., 2001, "Complexity Pursuit: Separating Interesting Components from Time Series", Neural Computation, vol. 13, pp. 883 – 898.

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

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

[21] Corchado, E.; Han, Y.; Fyfe, C., 2003, "Structuring Global Responses of Local Filters Using Lateral Connections", Journal of Experimental and Theoretical Artificial Intelligence, vol. 15(4), pp. 473 – 487.

[22] Corchado, E.; Fyfe, C., 2003, "Connectionist Techniques for the Identification and Suppression of Interfering Underlying Factors", International Journal of Pattern Recognition and Artificial Intelligence, vol. 17(8), pp. 1447 – 1466.

[23] Corchado, E.; Corchado, J.M.; Sáiz, L.; Lara, A., 2004, "Constructing a Global and Integral Model of Business Management Using a CBR System" First International Conference on Cooperative Design, Visualization and Engineering.

[24] Seung, H.S.; Socci, N.D.; Lee, D., 1998, "The Rectified Gaussian Distribution" Advances in Neural Information Processing Systems, vol. 10, pp. 350 - 356.

[25] Charles, D., 1999, "Unsupervised Artificial Neural Networks for the Identification of Multiple Causes in Data", Ph.D. Thesis, University of Paisley.

[26] T. Kohonen, 2000, "Self-Organizing Maps", Springer, 3rd edition, ISBN: 3-540-67921-9.