

# **Early warning system for the prevention and control of unauthorized accesses to air navigation services infrastructures**

A. Accettura<sup>1</sup>, G. Carelli<sup>2</sup>, F. Di Maio<sup>2</sup>, S. Donarelli<sup>1</sup>, F. Garzia<sup>1,3</sup>,  
M. Lombardi<sup>1</sup>

<sup>1</sup> *Safety & Security Engineering – SAPIENZA – University of Rome, Italy*

<sup>2</sup> *ENAV – Italian Provider for Air Navigation Services, Italy*

<sup>3</sup> *Wessex Institute of Technology, Southampton, UK*

## **Abstract**

Early warning systems are fundamental instruments for the management of critical situations since they are able to signal in advance any anomaly with respect to ordinary situations.

The purpose of this paper is to present an early warning system, based on artificial neural networks, for the prevention and control of unauthorized accesses to air navigation services infrastructure in Italy.

*Keywords: Air navigation services, early warning, neural networks.*

## **1 Introduction**

Air navigation services represent a very delicate mission for the security of air transports. This mission is made through integrated systems [1-4] that represent a critical infrastructure whose access, both from the physical and logical point of view, must be accurately checked and controlled. In fact, any unauthorized intrusion inside the control system could generate catastrophic consequences.

This research, whose field is the security of control of air transport, starts from the need to reveal any kind of unauthorized access into the sites which belong to the Italian Provider for Air Navigation Services (ENAV) both from the physical and logical point of view.

The proposed goal is reached using a proper artificial neural network (ANN) able to supervise the different accesses, and to give an early warning in case of

anomalies. Anomalies are defined in case of badge and computer username or password unauthorized use that are given by a proper Security Operation Centre (SOC).

The ad-hoc-designed ANN is trained using data such as badge owners, login codes, ENAV site number (ENAV has different sites located in different zones of Italy), date and hour of the access and so on, both in normal and early warning conditions.

Once the ANN is properly trained, it is able to analyse all the access data to the flight assistance system. Any time it reveals a suspect access, it immediately generates an early warning to the security operators to allow them to check the suspect accesses to avoid unauthorized intrusions that could negatively interfere with the normal activity of flight assistance.

The proposed ANN based system is capable to be trained constantly, so that it can learn new suspect access configurations, guaranteeing a high level of protection and security to the air navigation services provider system of ENAV.

The purpose of this paper is to illustrate the ANN based system, its design, its implementation and the interesting obtained results.

## **2 ENAV**

ENAV is Italian Provider for Air Navigation Services that is supervised by the Minister of Economy and Minister of Infrastructures and Transports.

It is composed by different central sites and numerous local sites such as 4 control centres (named ACC, located in Rome, Milan, Padua and Brindisi) and 40 airport structures, divided by tipology.

ENAV provides the following air navigation services (ANS):

- 1) air traffic services (named ATC, FIS, ALRS, ATAS);
- 2) aeronautical information services;
- 3) meteorological services;
- 4) communication, navigation and surveillance services.

## **3 The Security Operation Centre**

The Security Operation Centre (SOC) has been created and managed by ENAV that is the only European provider equipped with such as security governance structure.

The SOC is the physical and logical place where all the information (coming from all the controlled infrastructures) necessary to monitor the security converge.

The purpose of the SOC are:

- 1) to monitor, in proactive way, the security infrastructures by means a supervision and control activity of all the devices that ensure protection to ENAV personnel and to operative sites. It supervises and control all the systems/devices that performs air traffic control functions;
- 2) to prevent and manage incident in an efficient way;

- 3) to contribute to the government and management of security providing services and data related to the behaviour of security systems.

The SOC services are summarized in fig.1.










ACTIVITIES	DESCRIPTION	TIMEFRAME SERVICES
Real Time Device Monitoring	Real time monitoring of IT and IT related security events affecting IT infrastructures through specific tools able to detect and analyze potential security breaches or suspicious activities intended to exploit vulnerabilities	 H24 7x365
Incident Management	Processes and actions to deal with security incidents	 H24 7x365
Vulnerability Assessment	Continuous vulnerability assessment through specific indicators and controls	 9:00 – 18:00 mon-fri
Security Intelligence	Conducted in a transparent and continuous manner, information sharing	 9:00 – 18:00 Mon-Fri
Policy Management & Enforcement	Managing rules both for security devices and for personnel	 9:00 – 18:00 Mon-Fri
Technical & Executive Reporting	Analysis support and actions with the purpose of enhancing decision management	 9:00 – 18:00 Mon-Fri
Policy Compliance	Verification of policy (both laws/regulations and internal rules, referring also to best practices.	 9:00 – 18:00 Mon-Fri
Fault Management	Troubleshooting and support for contingency planning	 H24 7x365
End Point Protection	Security services for endpoints	 9:00 – 18:00 Mon-Fri

Figure 1: SOC services

SOC structure can be divided into two macro-areas:

- 1) SOC IT for the information, networks, and systems protection;
- 2) SOC PA for the centralized management of the physical security.

The SOC IT works in the internal perimeter of the E-Net and on the related services, aided by high-qualified personnel and properly differentiated according to professional profile, application field, working time.

The main unites that compose the SOC IT are represented by:

- 1) SOC SIG that supervises the information security of management information systems;
- 2) SOC ATC that supervises the ENAV information operative system and the security of the information of SOC devices;
- 3) SOC E-Net that manages and monitors the operative traffic on the E-Net (just IP traffic);
- 4) SOC IAO that manages the inter-domain events as second level for the control of the SIG, ATC, E-Net events in terms of quality assurance, resilience and forensic services.

## **4 Access control and early warning**

It is evident that it is very important to control the physical and the logical access to the system and every anomaly must be immediately signaled (early warning) to avoid that the intruder could make dangerous operation on the air navigation system.

An example of anomalous physical access is represented by the use of the same entrance badge in two different sites at the same time or in a too restricted time with respect to the physical distance of the two considered sites.

Is it therefore clear that it is very important to have an early warning system [3] that signals any anomalous access to the security personnel to activate all the necessary security procedures to prevent any attack to the air navigation system.

## **5 The early warning system**

The early warning system must check continuously every physical and logical access to the SOC and signal any anomalous access.

From this point of view, an Artificial Neural Network (ANN) that is capable to learn all the data related to normal and warning condition has been used.

The physical access to the sites is made by means of a badge while the logical access to the system is made through a login.

In case of physical access, the SOC receives the following data: <date>, <time>, < site identification code>, <user identification code>.

In case of logical access, the SOC receives the following data: <date>, <time>, < site identification code>, <username>.

It is therefore important to check the following couple of data:

- 1) badge – badge;
- 2) badge – login;
- 3) login – badge;
- 4) login – login;

to reveal any anomalous non matching between name of the operator, time, and physical distance between the sites.

The following normal/warning modality are considered;

- 1) entrance of the same user in the same site at any time interval (normal);
- 2) entrance of two different users in two different sites at any time interval (normal);
- 3) entrance of the same user in two different sites of the same city after a proper time interval depending on the physical distance between the two sites (normal);
- 4) entrance of the same user in two different sites after a too reduced time interval (warning).

## **6 The Artificial Neural Networks**

Artificial Neural Networks (ANN) find actually a lot of applications in different fields such as:

- 1) electronics: process control, machine vision, voice synthesis, linear and nonlinear modelling, signal analysis;
  - 2) robotics: trajectory control, vision systems, movement controller;
  - 3) telecommunications: image and data compression, noise reduction,
  - 4) security: face recognition, voice recognition and other biometrics applications, new sensors;
  - 5) defense: weapon steering, signal and image identification, radar and image signal processing, object discrimination and recognition;
- and other fields such as aerospace, insurance, banking, manufacturing, automotive, medical, financial, entertainment.

The common element of their field of applications is the need of classifying a given element as belonging to one or more given classes.

One of the main referring model for the reproduction of human intelligence is the so called 'Connectionism' that postulates the logic equivalence between any structured knowledge and a proper neural network. The Connectionism allows to develop a new form of artificial intelligence based on a sub-symbolic computation instead of the symbolic computation that represents the typical application field of the classical artificial intelligence. The Connectionism originates from the study of the working mechanisms of the central nervous system of biological organisms.

Human brain is composed by neurons that are cells whose purpose is represented by the information processing. Each neurons is connected with the other by means of a central body called axon and by numerous terminations called dendrites. The connection points between neurons are called synapses that show an excitatory behavior if they allows the electrical pulses to pass or an inhibitory behavior if they stops these pulses.

Each neuron behaves as an adder of the pulses generated by nearby neurons: if the sum overcomes a certain threshold the neuron actives letting the information to proceed along its path.

The connections between neurons can be modified allowing the memory effect to take place.

Artificial neural networks imitate this mechanism generating a knowledge database by means of the modification of the connections of a net that can learn from direct experience modifying its internal state to adapt to the solution of a particular problem.

The modeling of the behavior of neural networks is quite complex and generally uses the approach of the dynamic systems and the related concepts such as cycles, strange attractors and equilibrium points.

Neural networks are particularly useful when the law related to a certain phenomenon is not known in a deterministic way but it is necessary to reproduce it.

Neural networks are very useful when:

- 1) it is necessary to generalize the knowledge acquired on a restricted base to a wider base;
- 2) a certain situation changes with time;
- 3) data are not complete, uncertain or influenced by errors;

- 4) it is necessary a great tolerance to troubles or malfunctions;
- 5) it is necessary to find rapidly a heuristic solution to a particular problem;
- 6) a phenomenon rapidly changes and short adapting times are requested;
- 7) a high computational parallelism is requested;
- 8) a proper algorithm is not known;
- 9) qualitative or incomplete data are present;
- 10) the problem is data intensive instead of number crunching;
- 11) it is necessary to produce a knowledge for an expert system.

For all these reasons neural networks represent a useful and flexible tool for a lot of situations.

The elementary computation element of this kind of technology is represented by the neuron, that is a cell that receives one or more input values and produces one or more outputs that depend on the input values, as shown in fig 2.

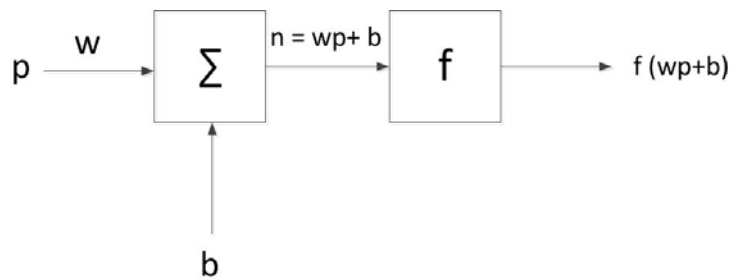


Figure 2: Single input neuron

Considering a single input - single output neuron, if  $p$  is the input and the  $w$  the weight, the product  $wp$  reaches the  $\Sigma$  unit where it is summed to a bias value  $b$ , that can be considered as an input of value equal to 1 and whose weight is equal to  $b$ . The computed quantity  $n=wp+b$  reaches the transfer function  $f$  that calculates the output of the neuron  $a=f(wp+b)$ .

The parameter  $w$ ,  $p$  and  $b$  are adjustable and they can be adapted so that the neuron exhibits an interesting or desired behaviour.

Therefore an elementary neuronal cell performs simple operations such as additions and multiplications which can be easily executed by low computation capabilities devices. Their strength relies on their organization in massively parallel architectures.

The elementary cells can be connected in different way to form a neural net that can be trained to do a particular job adjusting properly their weights and/or their biases (supervised learning) or letting it learn by itself (unsupervised learning that is typical of the self-organizing nets).

The transfer function of the neuron can have different expressions that are: step (symmetric and asymmetric), linear (with saturation or without saturation), sigmoidal (logarithmic or tangential), triangular, radial and others. If the neuron has more inputs:

$$p = [p_1, p_2, \dots, p_R] \quad (1)$$

each of them is multiplied by the weights:

$$\mathbf{w} = [w_{1,1}, w_{1,2}, \dots, w_{1,R}] \quad (2)$$

and the sum unit executes the dot product  $\mathbf{w}\mathbf{p}$ , adding the bias  $b$  to give:

$$w_{1,1}p_1 + w_{1,2}p_2 + \dots + w_{1,R}p_R + b \quad (3)$$

that is the argument of the output transfer function.

An example of multiple input neuron is shown in fig. 3.

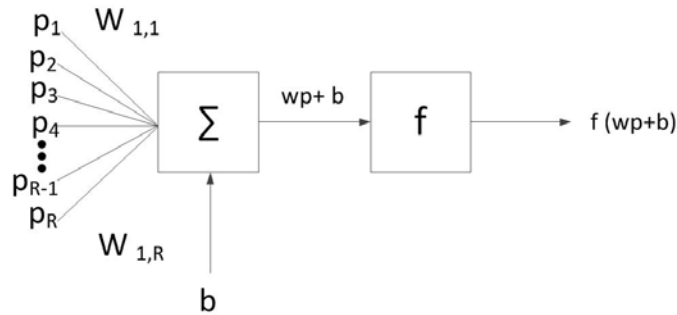


Figure 3: Multiple input neuron

Two or more multiple neurons can be combined to generate a layer of neurons. Considering a layer composed by  $S$  neurons, each element of the input vector  $\mathbf{p}$ , composed by  $R$  elements, is connected to each neuron input through the weight matrix  $\mathbf{w}$ . The  $j$ -th neuron weights properly its inputs, performing a dot product and adding the  $j$ -th bias to generate its scalar output  $n(i)$ . The various values  $n(i)$  taken together, form a vector  $\mathbf{n}$  composed by  $S$  elements. Each element of the vector  $\mathbf{n}$  represents the input of the transfer function of the relative neuron. At the output a column vector  $\mathbf{a}$  is obtained.

Generally the number of inputs  $R$  is different from the number of neurons  $S$ .

An example of a layer of neurons is shown in fig.4.

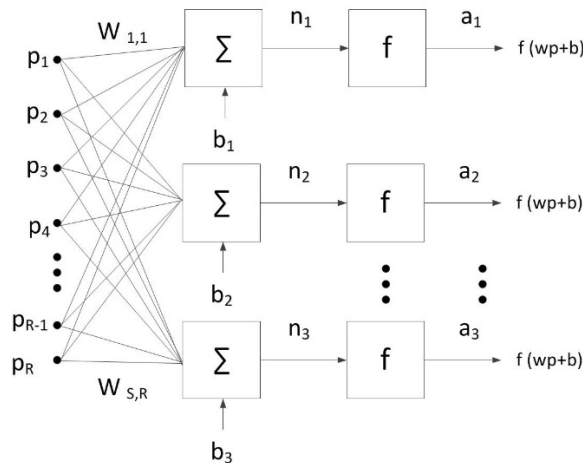


Figure 4: Layer of neurons

In a layer of neurons the weight matrix  $\mathbf{w}$  has the following form:

$$\mathbf{w} = \begin{bmatrix} w_{1,1} & w_{1,2} & \dots & w_{1,R} \\ w_{2,1} & w_{2,2} & \dots & \\ \dots & \dots & \dots & \dots \\ w_{S,1} & & \dots & w_{S,R} \end{bmatrix} \quad (4)$$

where the row indices indicate the destination neuron of the weight and the column indices indicate which source is the input for that weight. For example, the weight labeled with (3,2) expresses the strength of the signal from the second input element to the third neuron.

When we deal with a multiple layer net we deal with different weight matrixes  $\mathbf{w}$ , different bias vectors  $\mathbf{b}$ , and different output vectors  $\mathbf{a}$  each of them referring to the relative layer.

In this situation the first layer is called input layer, the network output is called output layer and the intermediate layers are called hidden layers.

Multiple layers nets can perform complex functions. For example a two layers net, where the first layer is sigmoid and the second layer is linear, can be trained to approximate any function with a finite number of discontinuities.

Networks with biases are able to represent relationships between inputs and outputs easier than networks without biases. In fact a neuron without a bias will always have a net input to the transfer function equal to zero when all of its inputs are zero while a neuron with bias can learn to have any net transfer function net input under the same conditions by learning an appropriate value for the bias.

An example of neural net with an input layer, an hidden layer and an output layer is shown in fig. 5.

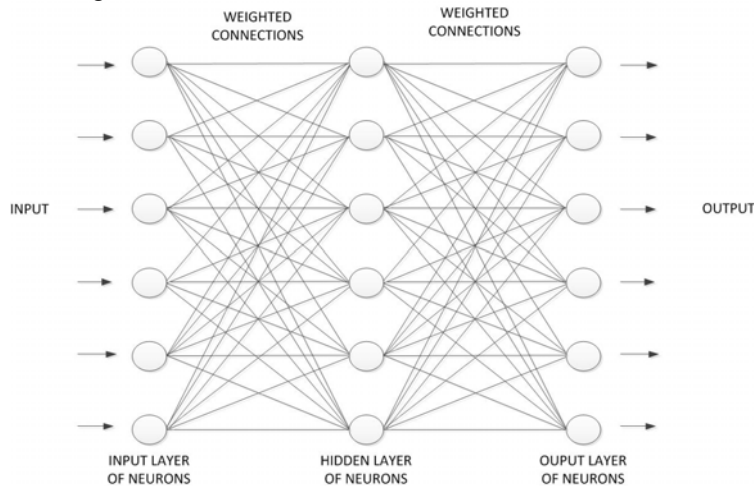


Figure 5: Example of neural network with an input layer, an hidden layer and an output layer.



## 7 The ANN used for the proposed system

The ANN used for our system is a Feed-Forward, characterized by the presence of one or more hidden layers that connect the input neurons with the output neurons. The learning algorithm is represented by the back propagation that calculates, at any learning step, the output and compares it with the expected value, trying to minimize the mean squared error (MSE) calculating the gradient of the error with respect to weight of the neurons to modify them successively. A sigmoid function has been considered as activation function of the neurons. Since only a single layer ANN has been considered, the critical factor to be focused is represented by the number of neurons the hidden layer.

## 8 Results

The ANN has been trained and then tested using a variable number of neurons of the hidden layer (8, 9, 10, 12, 13, 15), evaluating the performances of the different ANN by means of MSE that represents the most significant parameter for our purpose.

In fig. 6 the MSE results during the training phase obtained for different values of the number of neurons of the hidden layer are shown.

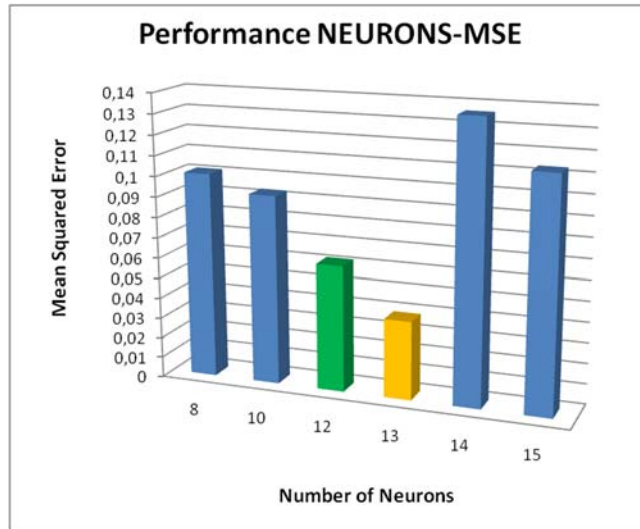


Figure 6: Mean squared error versus number of neurons of the hidden layer

From fig.6 it is possible to see that the ANN characterized by 13 neurons in the hidden layer is the network that presents the lower MSE and, for this reason, this is the network that has been used.

Once selected the number of neurons of the hidden layer, it is necessary to check the generalization capacity of the selected network.

The input data has been divided into 3 different groups:

- 1) training set;
- 2) validation set;
- 3) generalization test set.

Different attempts of division of the data set were made to find the optimal values that ensure the best generalization capacity that has resulted to be:

- 1) training set: 65% of data set;
- 2) validation set: 15% of data set;
- 3) generalization test set: 20% of data set.

## 9 Conclusions

Early warning systems are fundamental instruments for the management of critical situations since they are able to signal in advance any anomaly with respect to ordinary situations.

In this paper, an early warning system, based on artificial neural networks, for the prevention and control of unauthorized accesses to air navigation services infrastructure in Italy, has been studied, finding an optimal ANN capable of solving this delicate problem.

The system is very flexible since it can rapidly trained any time a variation in the users database occurs, due to the great flexibility of neural networks.

It is also very easy to be implemented since it needs a reliable PC, connected to the SOC network, where the ANN can run and perform its early warning functionality.

The system can obviously be further developed, studying new and more performing ANN architectures but this is out of the scope of the present work.

## 10 References

- [1] Garzia, F., Sammarco, E., Cusani, R., "The integrated security system of the Vatican City State", International Journal of Safety & Security Engineering, WIT Press, Vol. 1, No. 1, pp. 1-17, 2011.
- [2] Contardi, G., Garzia, F., Cusani, R., "The integrated security system of the Senate of the Italian Republic", International Journal of Safety & Security Engineering, WIT Press, Vol. 1, No. 3, pp. 219- 246, 2011.
- [3] Garzia, F., Cusani, R., "The integrated safety/ security/ communication system of the Gran Sasso mountain in Italy", International Journal of Safety & Security Engineering, WIT Press, Vol.2, No.1, pp. 13-39, 2012.
- [4] Garzia, F., Sammarco, E., Cusani, R., "Vehicle/people access control system for security management in ports", International Journal of Safety & Security Engineering, WIT Press, Vol.2, No.4, pp. 351-367, 2012.