Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.5 No.1, 2016, pp.21-24

DOI: https://doi.org/10.51983/ajcst-2016.5.1.1762

Information Security and Computer Security Using Neural Networks and Artificial Human Immune System

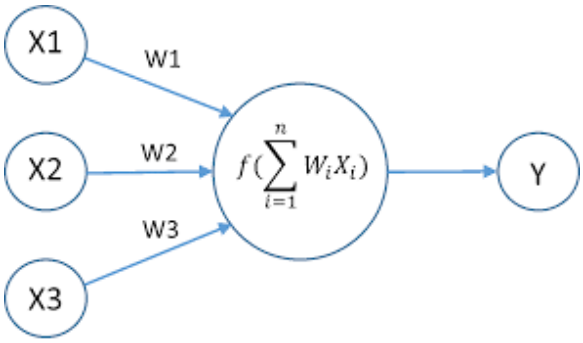
S.Senthil kumar[1] and R.Kanakaraj[2]
Assistant Proessor,
Department of Commerce with Computer Applications
Dr.SNS Rajalakshmi College of Arts and Science (Autonomous), Coimbatore, Tamil Nadu, India
E-mail: ssksnsmca@gmail.com
(Received 20 February 2016; Accepted 18 March 2016; Available online 28 March 2016)

Abstract **- Human beings are involved in the care and repair of computer systems at every stage in their operation. This level of human involvement will be impossible to maintain in future. Biological and social systems of comparable and greater complexity have self-healing processes which are crucial to their survival. An immune system needs to be cognizant of its local host's current situation and of its recent history; it must be an expert in intrusion detection. The body's immune system deals with threats to the operation of the body using a number of pro-active and reactive systems. Additional tasks need to be devoted to protecting and maintaining a computer with an immune system so that human intervention can be minimized. Whether the root cause of the errors is faulty programming or simply a lack of foresight, human intervention is required in computing systems with a regularity which borders on the embarrassing.With an immune system, a computer could detect problem conditions and mobilize resources to deal with them automatically, letting the machine do the work. Although the phrase immune system' would make many people think immediately of computer viruses, there is much more to the business of keeping systems healthy than simply protecting them from attack by hostile programs. If one thinks of biological systems or other self-sufficient systems, such as cities and communities, some of the most critical subsystems are involved in cleaning up waste products, repairing damage and security through checking and redundancy. It would be unthinkable to do without them.**
Keywords: Biometric, Neural Networks, Artificial Immune System

I.NEURAL NETWORKS

A neural network (NN) is a parallel distributed processing (PDP) architecture that is modeled after the working of the brain. It can perform computations, in particular classification of inputs, and provides an example of an alternative model of computation compared to the serially and centrally based computations of standard computing systems.

Our brains consist of many (about 10 billion) simple cells called neurons. Each neuron consists of a cell body, an axon (an elongated "transmission line" through which chemical signals can travel), and many dendrites (a tree-like structure of many branching "tentacles"), which end in synapses which form connections with the axons of other neurons. Simply put, each neuron receives inputs (the presence or absence of signals) from other neurons through the synaptic connections, which travel down the dendrites to the cell body. Here, the inputs are "added up", and if a certain threshold is reached the neuron sends out a signal itself through its axon, which is then forming an input to yet other neurons which are connected to its axon. However, not all synaptic connections are equal. Some are stronger than others, and so some inputs have a higher "weight" than others. Learning is achieved by adjusting the strengths (weights) of existing synaptic connections, or by creating new or deleting old connections.



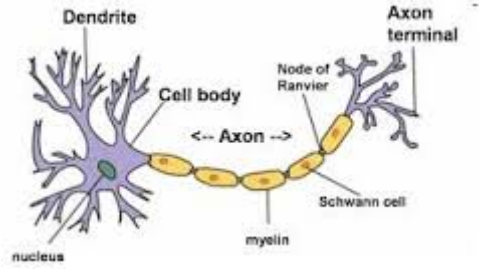


Fig. 1 & 2 Simplified model of a real neuron

A neuron receives inputs (x_i) from other neurons, which are weighted ($w_{i)}$ and then added (y). The output of a neuron is a function f (y) of this weighted sum of inputs, and can in turn form the input to other neurons In the simplest case, each input can be either 0 (absence of signal) or 1 (presence of signal), and the output function is a step function such that the output is 0 if the weighted sum of inputs is below a certain threshold value, and 1 if it is above the threshold value. In more realistic cases, the inputs and outputs are real valued numbers within some range, and the output function is for example a sigmoidal shape.

Any number of such neurons can be connected to each other to form an artificial neural network. A standard network architecture that is often used is a feed forward network. In such a NN, there is one layer of input neurons, one or more layers of "hidden" neurons, and one layer of output neurons, as illustrated in the figure on the next page. The neurons in the input layer are initialized with some input pattern, and the outputs from this layer go "forward" and serve as inputs to the first hidden layer. These neurons then produce their outputs which serve as inputs to the next hidden layer (if present), until the final, or output, layer is reached. The state of the neurons in the output layer can then be interpreted as the "answer". For example, in classification problems, if the state of the first output neuron is 1 and that of the second one is 0, the input belongs to one class. If their final states are reversed (i.e., 0 and 1, respectively), then the input belongs to the other class (assuming there are two classes into which to partition the inputs). Other network architectures are of course also possible, such as recurrent networks, where connections can feed back to previous layers as well, or grid networks, where the neurons are arranged in a grid with connections between neighboring neurons.

Given some network architecture, it is not directly obvious how to set the weights on the connections to get a certain network behavior. However, several training algorithms have been designed to optimize these weights. The main idea of these algorithms is to repeatedly present the network with example inputs for which the correct answer is known. The weights in the network are then updated depending on the amount of error between the correct answer and that given by the network. This is repeated until no more errors are made, or the amount of error falls below a certain threshold. The network can now be said to have learned the given task. At the next stage, the network can be used to perform the task on new inputs which it might not have seen before.

A.Applications of Neural Networks in Fingerprint Recognition

One area where neural networks have become very popular is image processing, such as pattern recognition and classification, noise filtering, edge detection, etc. As an application in biometrics for security, they can be used successfully for fingerprint recognition. Fingerprint recognition is often split up in two stages: (1) feature extraction, and (2) classification.

In the first stage, certain features from a fingerprint image are extracted, such as ridge directions, arches and whorls, delta points, etc. (for a more detailed overview. see for example [5]). In the second stage, these features are used to recognize (or classify) the given fingerprint image.

Neural networks have been applied successfully in both of these stages, often giving rise to high correct classification rates and low false rejection rates, and frequently outperforming more traditional methods (see for example [6], [7], [8], [9], and [10]). Furthermore, neural networks can be used similarly for other image recognition tasks in biometrics security, such as retina or iris scan classifications, or for voice recognition.

II.ARTIFICIAL IMMUNE SYSTEMS FOR COMPUTER SECURITY

A very recent idea that is still being developed is that of building a computer immune system. The task of such a system is to provide computer and network security based on the workings of the human immune system. This section first presents a high-level and somewhat simplified overview of the human immune system. A good introduction to this topic can be found in [11]. Next, an example of an implementation of a simple computer immune system is given to illustrate the applicability of the idea.

A.The human Immune System

The human immune system is a complex and multi-layered system. The part that is of most interest here is the adaptive immune response. A brief overview of this is given below, with many details left out. However, the general properties of this part of the immune system serve as a starting point for the design of an artificial immune systems for computer and network security.

The human body consists of many different types of molecules (mostly proteins), which are referred to as "self' everything else, including things that make us ill, is referred to as "non-self'. So, the main task of the immune system is to distinguish "non-self' from "self", and trigger a response whenever "non-self' proteins are detected. However, this is not an easy task as there are an estimated 1016 "non-self" proteins that the immune systems needs to recognize, compared to about 105 "self" proteins. The way the immune system solves this problem is by using a dynamic and distributed system. At any time, many "detector" cells, including so-called T-cells, circulate through our bodies. These cells mature in an organ called the thymus, where they are exposed to most of the "self' proteins that make up our bodies. If any of the maturing T-cells binds to any of these "self' proteins, that T-cell is eliminated. So, the only T-cells that leave the thymus are those that do not bind to "self' proteins. Consequently, if a matured T-cell does bind to a protein, it means this must be a “non-self protein”, and an appropriate immune response will be triggered. However, not all T-cells are able to bind to (or "recognize") all possible "none self' proteins, but some T-cells bind to some "non-self' proteins, other T-cells to others, etc. In this way, the immune system is a distributed system.

It is also dynamic, as T-cells are continuously replaced through a genetic process including variation (or random "mutations"). This way, the set of "non-self" proteins that the immune system is able to recognize, changes over time. Since it is impossible to recognize all possible "non-self' proteins at any one time, this dynamic system is the next best solution. Furthermore, because of this, no two individuals will have exactly the same set of T-cells at any given time, so what might make me sick, my neighbor might be immune to, and vice versa.

Finally, the immune system also has a "memory". It is capable of remembering illness-causing "non-self' proteins (antigens), so that the next time an individual gets infected with the same antigen, it is recognized immediately and an appropriate immune response can be triggered, preventing the actual illness from occurring again.

B.Immune System includes

The immune system comprises a battery of cells in almost every bodily tissue which have evolved to respond to violent cell death, both fighting the agents of their destruction and cleaning up the casualties of war: B-cells, T-cells, macrophages and dendritic (branching like a tree)cells to name but a few. Antigens are cut up and presented to T cells. This activates the T cells, priming them to attack any antigens which they bump into. B-cells secrete antibody molecules in a soluble form. Antibodies are one of the major protective classes of molecules in our bodies. Somehow the immune system must be able to identify cells and molecules which threaten the system and distinguish them from those which are the system.

The canonical theory of the immune system is that lymphocytes discriminate between self and non-self [17, 18, 19, 20, 21] (part of the system or not part of the system). This theory suffers from a number of problems to do with how such a distinction can be made. Foreign elements enter our bodies all the time without provoking immune responses, for instance during eating and sex. The body has its own antigens to which the immune system does not respond. This leads one to believe that self/non-self discrimination as a human concept can only be a descriptive approximation at best; from a computer viewpoint it would certainly be a difficult criterion to program algorithmically. Recent work on the so-called danger model [22] proposes that detector cells notice the shrapnel of non-programmed cell death and set countermeasures in motion.

C.Computer Immunology

Forrest and students were some of the originators of using principles from the human immune systems to design an intrusion detection system for computers and networks [12], [13]. In particular, in [14] they show the results of a basic implementation based on scanning short sequences of system calls. Briefly, the idea is as follows. In the first stage, a database of system call sequences during "normal" behavior is built. This database thus contains the sequences that constitute "self'. In the next stage, system call sequences are scanned during system operation that might contain intrusion attempts. These sequences are then compared to the available database, and any sequence that is not present in the database ("non-self") triggers an "alarm". This way, abnormal behavior can be easily detected, and appropriate actions can be performed if necessary.

Obviously, the databases containing normal behavior have to be updated frequently. For example, adding new users or software and hardware to the system will change the normal behavior, or a user's behavior might change over time (different tasks, different priorities, etc.). However, with this design, the intrusion detection system becomes more adaptive, as it is capable of recognizing abnormal behavior that has not been observed before. In other words, the system can identify, for example, new viruses or new attacking mechanisms, without the need for downloading new virus "signatures" from some central server first. Furthermore, different computers will have different databases of "self' behavior, so a virus that infects one computer, might not be able to infect every other computer.

This way, the network as a whole also has a better (distributed) protection.

The (small-scale) examples and simulation that have been implemented so far indicate the viability of these ideas, and show a promising future. Currently, the ideas and designs are still being developed further, and are also being picked up by others [15], [16]. Computer immunology and artificial immune systems are now an active area of research.

III.CONCLUSION

Traditional computing methods have several disadvantages, such as a lack of robustness and adaptability, and limited scalability. In contrast, biological systems, being mostly parallel distributed processing systems, are highly robust, adaptable, and scalable. Biologically inspired computing involves the design, implementation, and application of new computer methods and systems that incorporate these advantageous properties of biological systems. In this paper, a brief overview of biologically inspired computing has been presented, with some specific examples of how these methods can be used in information security in particular. Many of these methods have already been applied successfully, such as genetic algorithms and neural networks, and some are still being further developed, such as computer immunology. It is clear that the area of information security can benefit greatly from these new and exciting computing methods.

REFERENCES

[1] W.S.McCulloch and W.Pitts,"A logical calculus of the ideas immanent in nervous activity," Bulletin of Mathematical Biophysics, vol.5, pp.115-133, 1943

[2] R.P Lippmann,"An introduction to computing with neural nets,"IEEE ASSP Magazine,Vol.4.pp.4- 22,1987

[3] J.A.Anderson,Inroduction to Neural Networks,MIT Press,1995

[4] S.Haykin, Neural Networks: A comprehensive Foundation,Prentice Hall,1999.

[5] N.Ratha and R.Bolle,Eds., Automatic Fingerprint Recognition Systems. Springer Verlag,2004

[6] P. A. Hughes and A. D. P. Green, "The use of neural network for fingerprint classification," In Proceedings of the 2nd International Conference on Neural Networks, 1991, pp. 79-81.

[7] M. Kamijo, "Classifying fingerprint images using neural networks: Deriving the classification state, in Proceedings of the 3rd International Conference on Neural Networks,1993, pp. 1932-1937.

[8] C. L. Wilson, G. T. Candela, and C. I. Watson, "Neural network fingerprint classification,"Journal of Artificial Neural Networks, vol. 1 (2), pp. 203-228, 1994.

[9] H. V. Neto and D. L. Borges, "Fingerprint classification with neural networks," in Proceedings of the 4th Brazilian Symposium on Neural Networks, 1997, pp. 66-72.

[10] A Ceguerra and I. Koprinska, "Automatic fingerprint verification using neural networks," in roceedings of the International Conference on Artificial Neural Networks, 2002, pp 1281-1286.

[11] C. A. Janeway and P. Travers, Immunobiology: The Immune System in Health and Disease. Current Biology Ltd., 2nd edition, 1996.

[12] S. Forrest, S. A. Hofmeyr, and A. Somayaji, "Computer Immunology," Communications of the ACM, vol. 40 (10), pp. 88-96, 1997.

[13] A. Somayaji, S. A. Hofmeyr, and S. Forrest, "Principles of a computer immune system," in New Security Paradigms Workshop, 1998, pp. 75-82.

[14] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff, "A sense of self for Unix processes," in Proceedings of the IEEE Symposium on Computer Security and Privacy,1996.

[15] J. Kim and R Bentley, "The human immune system and network intrusion detection," in Proceedings of the 7th European Conference on Intelligent Techniques and Soft Computing, 1999.

[16] J. Kim and P. Bentley, "Towards an artificial immune system for network intrusion detection: An investigation of dynamic clonal selection," in Proceedings of the Congress on Evolutionary Computation, 2002, pp. 1015-1020.

[17] F. M. Burnet. The Clonal selection theory of acquired immunity. Vanderbilt Univ. Press, Nashville TN, 1959.

[18] F. M. Burnet and F. Fenner. The production of antibodies. Macmillan, Melbourne/London, 1949.

[19] J. Lederberg. Science, 1649:129, 1959.

[20] R. E. Billingham, L. Brent, and P. B.Medawar. Nature, 173:603, 1953.

[21] R. E. Billingham. Proc. Roy. Soc. London.,B173:44, 1956.

[22] P. Matzinger. ``Tolerance, danger and the extended family." Annu. Rev. Immun., 12:991, 1994.