[1] M. Meisel, V. Pappas, and L. Zhang. A taxonomy of biologically inspired research in computer networking. *Computer Networks*, 54(6):901 - 916, 2010. New Network Paradigms. [bib | DOI | http]

> The natural world is enormous, dynamic, incredibly diverse, and highly complex. Despite the inherent challenges of surviving in such a world, biological organisms evolve, self-organize, self-repair, navigate, and flourish. Generally, they do so with only local knowledge and without any centralized control. Our computer networks are increasingly facing similar challenges as they grow larger in size, but are yet to be able to achieve the same level of robustness and adaptability. Many research efforts have recognized these parallels, and wondered if there are some lessons to be learned from biological systems. As a result, biologically inspired research in computer networking is a quickly growing field. This article begins by exploring why biology and computer network research are such a natural match. We then present a broad overview of biologically inspired research, grouped by topic, and classified in two ways: by the biological field that inspired each topic, and by the area of networking in which the topic lies. In each case, we elucidate how biological concepts have been most successfully applied. In aggregate, we conclude that research efforts are most successful when they separate biological design from biological implementation - that is to say, when they extract the pertinent principles from the former without imposing the limitations of the latter.
>
> Keywords: Epidemic routing

[2] D. Miorandi, L. Yamamoto, and F. D. Pellegrini. A survey of evolutionary and embryogenic approaches to autonomic networking. *Computer Networks*, 54(6):944 - 959, 2010. New Network Paradigms. [bib | DOI | http]

> The term “autonomic networking” refers to network-level software systems capable of self-management, according to the principles outlined by the Autonomic Computing initiative. Autonomicity is widely recognized as a crucial property to harness the growing complexity of current networked systems. In this paper, we present a review of state-of-the-art techniques for the automated creation and evolution of software, with application to network-level functionalities. The main focus of the survey are biologically-inspired bottom-up approaches, in which complexity is grown from interactions among simpler units. First, we review evolutionary computation, highlighting aspects that apply to the automatic optimization of computer programs in online, dynamic environments. Then, we review chemical computing, discussing its suitability as execution model for autonomic software undergoing self-optimization by code rewriting. Last, we survey approaches inspired by embryology, in which artificial entities undergo a developmental process. The overview is completed by an outlook into the major technical challenges for the application of the surveyed techniques to autonomic systems.
>
> Keywords: Artificial embryogenies

[3] T. S. Sobh and W. M. Mostafa. A cooperative immunological approach for detecting network anomaly. *Applied Soft Computing*, In Press, Corrected Proof:-, 2010. [bib | DOI | http]

> Technology and biological systems have now bi-directional relation that each benefits from the other. Biological systems naturally enjoy many attractive features and inherent intelligence that fit in solving many research problems. The natural immune system as one of those biological systems is considered a good source of inspiration to artificial defense systems. It has its own intelligent mechanisms to detect the foreign bodies and fight them and without it, an individual cannot live, even just for several days. The new types of network attacks evolved and became more complex, severe and hard to detect. This resulted in increasing need for network defense systems, and especially those with unordinary approaches or with ability to face the dynamic nature of new and continuously changing network threats. In this work we investigate different AIS theories and show how to combine different ideas to solve problems of network security domain. An Intrusion Detection System (IDS) that apply those ideas was built and tested in a real-time environment to test the pros and cons of Artificial Immune System (AIS) and clarify its applicability. Also some investigation on the vaccination biological process is introduced. A special module was built to perform this process and check its usage and how it could be formulated in artificial life.
>
> Keywords: Danger Theory