Bio-inspired mechanisms for efficient and adaptive network security

Falko Dressler

Computer Networks and Communication Systems

University of Erlangen-Nuremberg, Germany

dressler@informatik.uni-erlangen.de

Keywords

bio-inspired networking, self-organization, network security, organic computing

Abstract

In recent years, many efforts have been made in developing algorithms and methodologies for building efficient network security mechanisms. The primary requirements are efficiency, adaptability, and scalability. Network security mechanisms are composed of several components. First, high-performance network monitoring entities are required allowing the analysis of transmitted data even in high-speed backbone networks. Secondly, algorithms to detect various kinds of threats have to be developed. Based on the monitored data, statistical anomaly detection methods and policy-based filters can be employed. Finally, the control loop must be closed by involving firewall devices against ongoing attacks.

Organic computing is attempting to build high-scalable architectures, which are self-organizing, self-maintaining, and self-healing. We try to study the processes in computer networks using mechanisms known from molecular biology as the key paradigm. This novel approach shows many similarities between computer networking and cellular mechanisms. Based on the knowledge about cellular metabolism, new concepts for the behavior patterns of routers, monitor systems, and firewalls can be deduced and the efficiency of individual sub-systems can be increased.

This work focuses on the area of network security as one research area with high demand for high-scalable mechanisms providing the needed functionality. We see the proposed mechanism as a generic approach for self-organizing, i.e. self-configuring, self-managing, self-healing, and adaptive solutions in computer networking.

1. Introduction

Looking for efficient network security mechanisms, questions on the organization of nowadays communication networks arrive. Such networks are composed of network nodes with different duties, e.g. routers for packet forwarding, firewalls for packet filtering, and monitoring probes for traffic analysis. A schematic overview to the network security architecture is shown in Fig 1.

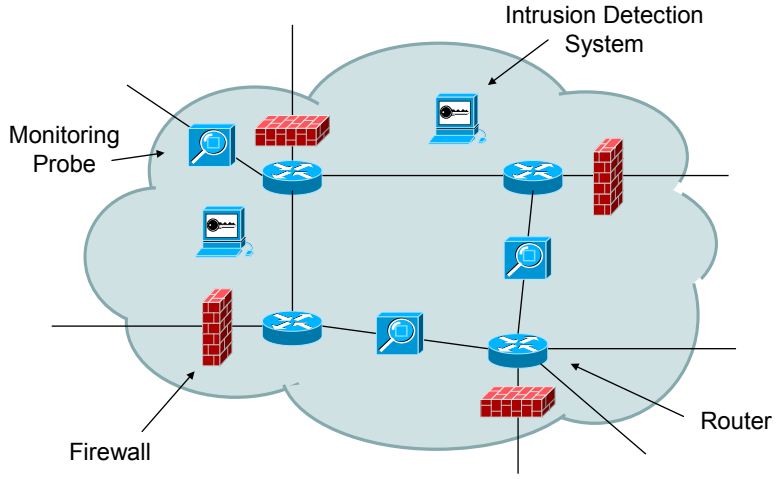

Fig 1. Schematic overview to the network security architecture

Recently, many efforts were made in creating network security mechanisms. Each singular component was enhanced in quality and performance. In the global context, efficiency, adaptability, and scalability are the primary requirements. Therefore, the interaction of all the single network nodes must be optimized in a way, that even without knowledge about the existing (available) neighbors the security in the network can be controlled.

Examples for the state-of-the-art security mechanisms are, first, high-performance network monitoring entities that allow the analysis of transmitted data even in high-speed backbone networks. Ideally, such monitors export the collected information using a standardized protocol such as IPFIX [2, 4] or PSAMP [6]. Based on the monitored data, statistical anomaly detection methods and policy-based filters can be employed. The most-known intrusion detection systems (IDS) are Snort [3], Prelude [1], and Cossack [11]. Typically, such IDS work on packet data from a single point in the network. Additionally, few attempts were made to build distributed, cooperating systems. An example for such a distributed approach is shown in [7]. Finally, the control loop must be closed by involving firewall devices against ongoing attacks. Firewall technology is available from numerous companies and also as open source software.

We address the mentioned issues in network security, i.e. the organization or management of the several network nodes using a bio-inspired approach. Organic computing [10] is attempting to build high-scalable architectures, which are self-organizing, self-maintaining, and self-healing. We try to study the processes in computer networks using mechanisms known from molecular biology as the key paradigm. This novel approach shows many similarities between computer networking and cellular mechanisms. Based on the knowledge about cellular metabolism, new concepts for the behavior patterns of routers, monitor systems, and firewalls can be deduced and the efficiency of individual sub-systems can be increased.

The rest of the paper is organized as follows. First, a structural comparison between organisms and network structures is provides which provides the basis for our evaluations. Secondly, the information exchange in cellular environments is detailed in order to discover the issues in network security which might be addressed using bio-inspired research. A conclusion summarizes the document.

2. Structure of organisms and computer networks

Before going on with the description of potentials in bio-inspired networking based on cell and molecular biology, a short overview to the state-of-the-art in bio-inspired engineering is given in the following.

Research on the utilization of biological mechanisms for engineering and computer science related fields started in the 1960ies with bio-inspired mechanisms, an artificial immune system, for virus detection. Until know, many papers on such topics were published basically focusing on the artificial immune system and on swarm intelligence. Examples are research on virus detection [9], intrusion detection [8], middleware platforms [12], and optimizations [5] in computer networks. Nonetheless, other areas such as evolutionary (or genetic) algorithms and neural networks are also of importance until now.

We are opening another area, the cell and molecular biology, for application in computer science. In Fig 2., a structural comparison of organisms and computer networks is shown. It can be seen that both show high similarities. Organisms are composed of organs, these of tissues, and, finally, of cells. An internet consists of network domains, (sub-)networks, and network nodes, respectively. Also, the intercommunication between the systems is similar. Information exchange between cells, called signaling pathways, follows the same requirements as between network nodes. A message is sent to a destination and transferred, possibly using multiple hops, to this target.

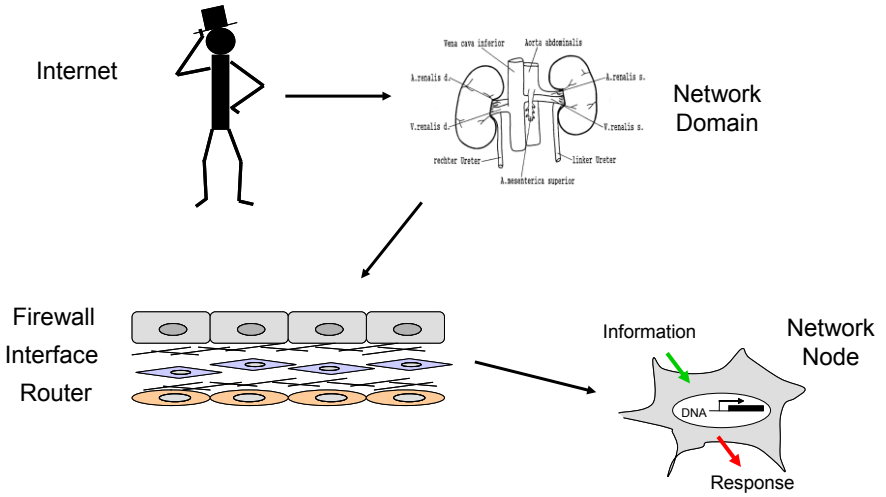

Fig 2. Structural comparison of organisms and computer networks

3. Cellular information exchange and adaptation to network security

The focus of this section is to examine the information exchange in cellular environments and to extract the issues in computer networks (focused on network security) which can be addressed by the utilization of these mechanisms.

From a local point of view, the information transfer works as follows. A signal reaches only cells in the neighborhood. The signal induces a signaling cascade in each target cell resulting in a very specific answer which vice versa affects neighboring cells. This process is depicted in Fig. 3. On the left side, a cell is shown with a single receptor that is able to receive a very specific signal and to activate a signaling cascade which finally forms the cellular response.

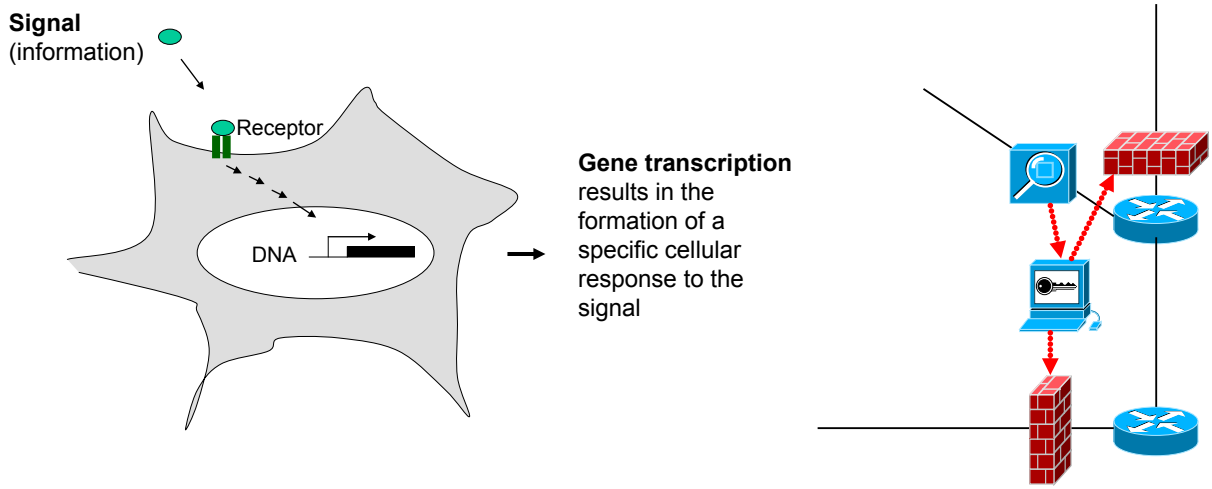

Fig. 3 Local information exchange: cellular environment (left); computer networks (right)

On the right side of Fig. 3, a network is shown consisting of a couple of network nodes. A monitor sends gathered packet data to an attached IDS. The firewalls are programmed with

rules that are the result of the analysis of the monitoring data. General issues to address in such a network are:

- Adaptive group formation
- Optimized task allocation
- Efficient group communication
- Data aggregation and filtering
- Reliability and redundancy

The remote information exchange works similar. As shown in Fig. 4, proteins are used as information particles between cells. A signal is released in the blood stream, a medium which carries it to distant cells and induces an answer in these cells which then passes on the information or can activate helper cells (e.g. the immune system). The interesting property of this transmission is that the information itself addresses the destination. Only cells with a very specific receptor are able to receive the information, i.e. the protein binds at the receptor.

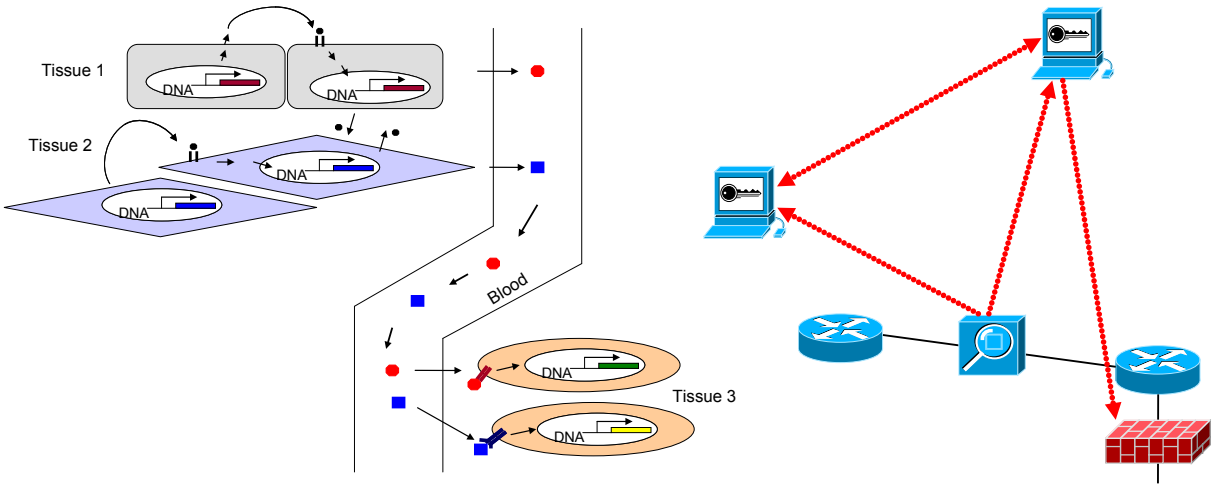

Fig. 4 Remote information exchange: intercellular (left); between network domains (right)

Corresponding issues in network security are for example:

- Localization of significant relays, helpers, or cooperation partners
- Semantics of transmitted messages
- Cooperation across domain borders
- Internetworking of different technologies
- Authentication and authorization

The lessons to learn from biology are the efficient response to a problem, the shortening of information pathways, and the possibility of directing each problem to the ideal helper component. Therefore, the adaptation of mechanisms from cell and molecular biology promises to enable a more efficient information exchange. Additionally, issues of task allocation and group communication are directly addressed by the introduced capabilities.

4. Conclusions and further work

Comparing cellular structures with computer networks, we always find similar structures. Specific signaling pathways are directly adaptable to information exchange in network security environments and adaptable for other communication relationships. Self-organization of complex operations becomes possible using bio-inspired mechanisms.

Our future work concentrates on the identification of general applicable solutions, the development of new algorithms for communication in highly distributed environments, and simulations and tests in lab environments.

References

[1] M. Blanc, L. Oudot, and V. Glaume, "Global Intrusion Detection: Prelude Hybrid IDS," Technical Report, 2003. (http://www.exaprobe.com/labs/downloads/Papers/Prelude.pdf)

[2] P. Calato, J. Meyer, and J. Quittek, "Information Model for IP Flow Information Export," draft-ietf-ipfix-info-03.txt, February 2004.

[3] B. Caswell and J. Hewlett, "Snort Users Manual," The Snort Project, Manual, May 2004. (http://www.snort.org/docs/snort_manual.pdf)

[4] B. Claise, "IPFIX Protocol Specifications," Internet-Draft, draft-ietf-ipfix-protocol-05.txt, August 2004.

[5] G. Di Caro and M. Dorgio, "AntNet: Distributed Stigmergetic Control for Communication Networks," Journal of Artificial Intelligence Research, vol. 9, pp. 317-365, December 1998.

[6] T. Dietz, F. Dressler, G. Carle, and B. Claise, "Information Model for Packet Sampling Exports," Internet-Draft, draft-ietf-psamp-info-02.txt, July 2004.

[7] F. Dressler, G. Münz, and G. Carle, "Attack Detection using Cooperating Autonomous Detection Systems (CATS)," 1st IFIP TC6 WG6.6 International Workshop on Autonomic Communication (WAC 2004), Berlin, Germany, Poster, October 2004.

[8] S. Hofmeyer and S. Forrest, "Architecture for an Artificial Immune System," Evolutionary Computation, vol. 8, pp. 443-473, 2000.

[9] J. O. Kephart, "A Biologically Inspired Immune System for Computers," Proceedings of 4th International Workshop on Synthesis and Simulation of Living Systems, Cambridge, Massachusetts, USA, 1994, pp. 130-139.

[10] C. Müller-Schloer, C. von der Malsburg, and R. P. Würtz, "Organic Computing," Informatik Spektrum, vol. 27, pp. 332-336, August 2004.

[11] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, "COSSACK: Coordinated Suppression of Simultaneous Attacks," Proceedings of DARPA Information Survivability Conference and Exposition, Washington DC, USA, April 2003.

[12] M. Wang and T. Suda, "The Bio-Networking Architecture: A Biologically Inspired Approach to the Design of Scalable, Adaptive, and Survivable/Avilable Network Applications," Proceedings of 1st IEEE Symposium on Applications and the Internet (SAINT), San Diego, CA, USA, January 2001.