MODELING AUTONOMIC MONITORING AND CONTROL FOR IoT SYSTEMS

Zenon Chaczko[(a)], Ryszard Klempous[(b)], Jan Nikodem[(c)]

[(a)] Faculty of Engineering and Information Technology,University of Technology, Sydney,
15 Broadway, Ultimo, NSW, Australia, 2007.
[(b), (c)]Institute of Computer Engineering, Control and Robotics, Wroclaw University of Technology,
11/17 Janiszewskiego Street, 50-372 Wroclaw, Poland

[(a)]Zenon.Chaczko@uts.edu.au, [(b)]Ryszard.klempous@pwr.wroc.pl, [(c)]Jan.Nikodem@pwr.wroc.pl

ABSTRACT
This paper introduces a bio-inspired approach for development of collective intelligence based computational models. These models are suitable for autonomous sensing, monitoring and control strategies for ambient systems based on Internet of Things technologies. Authors discuss issues and challenges related to modelling, design and implementation of a large scale, Internet of Things based smart system infrastructure such as smart office building, airport, public transport, etc. Additionally, various autonomous management strategies that anticipate variable levels of resource usage in Internet of Things systems are being presented

Keywords: bio-inspired modelling, autonomics, Internet of Things, large-scale infrastructure

1. INTRODUCTION

The management of complex, heterogeneous and distributed (network based) system composed of collaborating, sensors, actuators and robotic devices is a challenging task; and unless done effectively can significantly reduce the overall efficiency; degrade capacity to perform various functions as well as limit access to available resources in remote, dynamic and often hostile environment. This is particularly true in heterogeneous, network based environments as the actual structure of the network based system can change depending upon such disparate factors as the application tasks, communication links, hardware, topology and geography and environmental conditions. The software intensive, autonomous (Ishida 1997) and collective intelligence (Por 1995, Brown & Lauder 2000, Kennedy 2006, Kaiser et al. 2010 infrastructure for IoT system aims to lay the foundations for developing service-oriented and real-time system. These systems can be used for monitoring and control applications where containment of dangerous events or re-collection of available resources is critical. Apart of the on-board computer(s) to support the system's high functions, the system's' infrastructure is built as a highly reconfigurable network of sensors, actuators and robotic devices. The ability to adapt to the changing environments requires a step change in the design approaches. The key research challenge is to provide flexible resource management and data access solutions that are effective in a large-scale, heterogeneous system network. The outcomes of the initial design will enhance the position of the AI group to become not only an advisory body but to ensure a sustainable vision for future development of advanced engineering and co-evolution of and open hardware and software platforms. The modelling and simulation of software intensive systems (Bruzzone and Longo 2005) need to consider the high level decision making and system wide functions as well as individual (autonomous) computational and communication facilities (i.e., localisation, navigation, control and communication) that reside at the systems' lower levels.

The system requires the global information management and application software development facilities that are implemented in higher level programming languages. The development of a prototype required a set of high performance management solutions; middleware and software component frameworks that are able to facilitate the development of a network based, infrastructure oriented and embedded software for swarms (Bonabeau et al. 1999) of sensors, actuators and robotic devices. This paper is aimed at addressing the problem of dynamically managing the network of sensors, actuators, robots and various other associated resources so that specified communication links, data rates and priorities as defined by the real-time management system can be achieved (Das et al. 2004). This entails a development of infrastructure oriented software and algorithms for construction and simulation of real-time, mission critical solutions in resource constrained and possibly ambient environments.

2. AUTONOMICS

The concept of autonomics can be perceived as a capability of software systems to perform and manage their operations completely by themselves or only with a minimal level of human intervention. Autonomic systems, including Internet of Things (IoT) systems by adopting the concepts of autonomics are capable of self-managing all its elements and data communication links. In autonomic scenarios, wireless communication

is complex and requires designers to consider a number of problems related to sensor and actuator localisation, clustering, routing, energy management as well as various constraint conditions related to transmission collisions, multipath interference, obstructions that adversely impact the data throughput of high bandwidth communications robustness, reliability and scalability (Loureiro and Ruiz 2007). In order to face the challenges related to implementation of autonomic functions in IoT we propose a model of biomimetic IoT system that is characterised by the following fundamental properties:

2.1. Self-organisation

The phenomenon of self-organisation is pervasive in natural systems (Kauffman 1995), (Bak 1996). It can be defined as a system's tendency to evolve into a more organised state in the absence of external factors as a response to changes in the system's environment; It can be also perceived as a collective and coordinated process in which system's components achieve a higher level of organisation while interacting with other elements as well as and with the environment. Software systems incorporating a collective made of a number of components communicating, interacting among each other and with the environment. Collectively these elements can perform various tasks as a group, coordinating their tasks and activities to obtain a higher level of efficiency. The sum of dynamic behaviour arising due to interactions between different parts of the IoT based system could result in a coherent behaviour of the system as a whole. The IoT sensitivity relies on capability of software services to perform changes even if the value of an observed or control parameters is modified by a small value only. Since by principle, the self-organisation properties cannot be predetermined, the IoT system facilitated by software infrastructure can evolve to a new configuration that is compliant with the global system functions and environmental constraints. The robustness of the self-organising system can be then measured by a rate at which the system in its newer configuration is able to detect and handle its faults.

2.2. Self–shaping

A system's self-shaping property can be defined as allometric and scale-invariant (power-law scaling) characteristics of a system that addresses various aspects of self-adaptation and self-optimisation (McMahon & Bonner 1983), (Niklas 1994), (Phillips 2006). It can be interpreted as the capability of the system to alter or adjust its structure, size and rates of metabolic processes according to its varying internal and external stimulations (or events). In resource constrained IoT networks there is a requirement for software to be able to self-modify the network shape, adapt to variable levels of available resources and changes in the environment. In order to promote the system emergent properties such as robustness, or survivability of the IoT, this needs to occur by respecting scale-invariant relations.

In order for IoT software system infrastructure to support management of the IoT according to varying levels of available resources, tasks and changes in the environment we need to model, design and then implement the self-shaping (i.e. self-modification of the network topology) function requirement. It is suggested that this new type of the system property can be ensured if we follow allometric laws (Darveau et al. 2002, Chaczko 2009) that are often pertinent to living systems (McMahon and Bonner 1983), (Calder 1984), (Bejan 2002).

2.3. Self-adaptation and self-healing

The self-adaptation property can be seen as a capability of a system to modify/alter or adjust its internal structure or/and behaviour according to varying conditions in its surrounding.

The self-healing is to be perceived as a capability that allows automatically detecting, localizing, diagnosing and repairing failures. The process of self-healing is adaptive, fault-tolerant and inter-dependent with the mechanism of self-monitoring.

2.4. Robustness and resiliency

Robustness (fault tolerance) can be perceived as a capability of the system to resist or tolerate noise, disturbances, faults, stress, modification in system architecture (both structure and behaviour) or changes in the ecosystem without negatively affecting the system's functions or having long term effects on its structure and behaviour.

The property of resiliency can viewed as capability to absorb and even utilise (frequently with advantageous results) noise, disturbances and changes that attain them, in order to sustain and persist without any qualitative changes in the architecture of the system.

IoT for resource constrained systems need to be flexible to change and resistant to damage or faults; the systems should be able to self-modify their past behaviour and adapt to newly allocated tasks, changes in levels of available resources or changes in environment. IoT based systems can be perceived as being robust, if they would be able to tolerate failures, non-cooperative behaviour or conflict relation among its components. This can be achieved by including software functions that apply genetic mutation and reproduction to seed autonomic properties in IoT.

2.5. Cooperativeness

Characteristics of cooperativeness are perceived as a system's capability to stimulate collective and cooperative interactions among its components. Components can perform various tasks in teams, coordinating their activities to obtain an optimal efficiency. In reality, there are various degrees of cooperation/competitive (in resource constrained situations) behaviour at place. The sum of dynamic

behaviour arising from cooperative interactions between different parts of the system could decide about coherent behaviour and robustness of the whole system. Thus robustness of a system can be measured as a rate at which its components (resources) are repaired or replaced against the rate they diminish.

3. APPROACH AND METHODOLOGY

The software methodologies and tools are core aspects of all networked oriented system infrastructure software. These infrastructure oriented software are implemented to efficiently combine, manage data and control robotic swarms. At some stage, infrastructure oriented software is to play of enormous significance in such areas as: ambient management system's infrastructure management, environment monitoring, adaptation/articulation of all major parts, sensing and actuation, security and safety, education as well as many other areas that depend critically upon software technology. However, building application that make best use of AI and IoT technology in terms of practicality and economics (including time to deploy) cannot be fully realised without a consensus by majority of application developers on adequate methodologies and tools. In the context of remote management of infrastructures, such methodologies and tools for robotic network systems can significantly improve development life cycle the value of embedded devices and sensor infrastructure, reduce the cost of information management and offer technically and economically significant as well as viable implementations to many participating institutions.

3.1. Scope

The scope for cross disciplinary knowledge advancements when discussing hardware and software of architecture is significant. First and foremost is the advancement associated with the application of autonomics and information AI to improve the engineering methods of analysis, simulation and prediction. Second is the advancement associated with the development of cost effective and robust network architecture for local and remote operations. Third is the advancement associated with the application of biomimetic and AI paradigm that will enable the sharing of resources for multiple infrastructure oriented software concurrently. Owing to the richness of the field and the number of open problems in the domain, there is significant scope for several serendipitous advancements in the knowledgebase of several disciplines. The following new methodologies and technologies were being developed in the course of the discussed project:

1. New design paradigms for infrastructure networks with distributed processing and AI for autonomic robotic network infrastructure management.
2. New and open Service Oriented Architectures that support access to the fused/processed remote sensor/actuator information by possibly multiple applications.
3. Advanced infrastructure oriented software tools for development and integration of real time, context sensitive and proactive software Infrastructure for mission critical robotic networks/infrastructures.

3.2. Approach

The presented research approach involves the following stages:

1. Development of a working definition of Service Oriented Architecture-like infrastructure software for IoT based and embedded robotic systems. The output of this stage might be a document describing the architecture and how it applies to the needs of ambient management system. The document will include such high level design components as: Service Configuration, Service Activation, Fault Data Collection, Performance Data Collection and Usage Data Collection modules.

2. Identification of the mechanisms, policies and possible parameters for enforcing control and management of individual robotic drones and their swarms. Outcome of this stage is a design document identifying the policies, algorithms and equipment parameters that can be used for controlling and managing ambient management system.

3. Modelling, design and development of algorithms for management execution of real-time functions of ambient management system architecture in the test-bed environment. During this stage a prototype of performance management software for the equipment currently available in the lab has been developed.

4. Development of suitable algorithms for task allocation within individual embedded devices/motes and across groups of these devices. A small scale simulation environment has been used to test different resource allocation techniques. In this phase, simple search techniques were applied. More sophisticated and more scalable resource allocation techniques will be the focus of the future work.

The modelling and the development of the IoT based demonstrator allows for testing and validation of various autonomic behaviours that could be applied in various user environments. The main objectives is to demonstrate dynamic/adaptive modifications in device resource settings to meet a given control priority setting. This includes the management and decision-making software for the current ambient management environment. The demonstrator can be used to show how the autonomic management and decision making

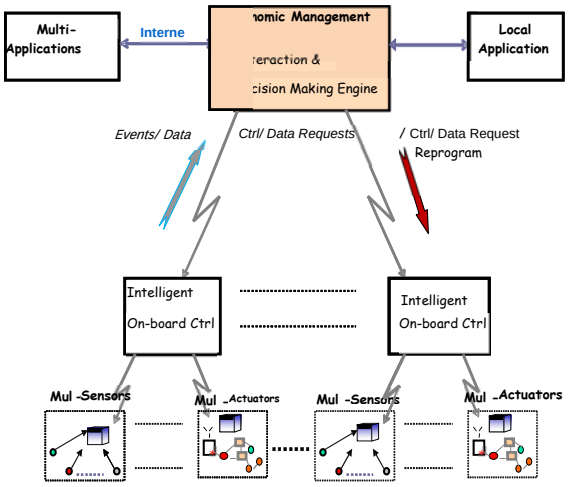

Figure 1: Conceptual architectural model of IoT infrastructure

system works in dynamic environment as well as to test the performance of such a system.

4. MODELLING SYSTEMS BASED ON COLLECTIVE INTELLIGENCE

4.1. The architecture for ambient systems

The main driver requirement for modelling systems based on collective intelligence was to develop an open source, cost effective and reliable architectures which would support a rapid development, validation and test of various autonomic concepts and user applications. Infrastructure hardware and software is to make the best use of emerging computer and network device platforms in order to facilitate information processing at the individual IoT motes, local level controllers (intelligent on-board computers) and the central computer(s). One of the key advantages of the proposed biomimetic model approach is that by processing information locally, the system can reduce the amount of data that needs to go on the networks. More importantly, there would be no need to send all that irrelevant or redundant data through the network and thus burdening the transaction requirements of the systems. In line with this view, the proposed architectural model allows the processing to move from wherever it is to a point closer to the sensors and actuators. This has a potential to fundamentally transform the efficiencies associated the computing and network support infrastructure. The proposed system architecture (hardware and software) has been developed for multi-sensor/actuator, multi-application environment of the swarm-like, human nervous modeled system (Fig. 1 and Fig. 2.)

Although most of the processing may be done closer to source, still one needs an efficient Internet and Web Services like and possibly Cloud Computing (grid middleware) access. The proposed remote information management approach is illustrated in Fig 2. Web user logs into the web system to request services that include the main functionalities of the web system such as view, analysis and control of required information. The web browser transfers the user request to the web server. The web server sends the service request to the information server for information. The information is retrieved from the data storage server. In principle the data can be embedded in the intelligent on-board controller (IOBC). The data server processes the information using heuristic techniques, returns the results to the data storage server, and then returns the data to the web server for the display on the web pages. The web user interacts with the web pages for the next service request.

4.2. Biomimetic model for IoT

In IoT base systems, low cost sensors and actuators with embedded computing and communication capabilities are enabling a new paradigm where sensors and actuators can share resources, just like the way computers are able to form a grid to share the computing power. The discussed ambient management system architecture, at presentation and business logic layers would still require a significant computational power. Hence, the system's higher level functions need to be provided with a dedicated on-board CPU(s) (Linux box). While, the ambient management system can rely on Web services and Cloud computing infrastructure (grid middleware). The vision for the model is to push the advancement of a modern IoT solution by enabling sensors and actuators to form a

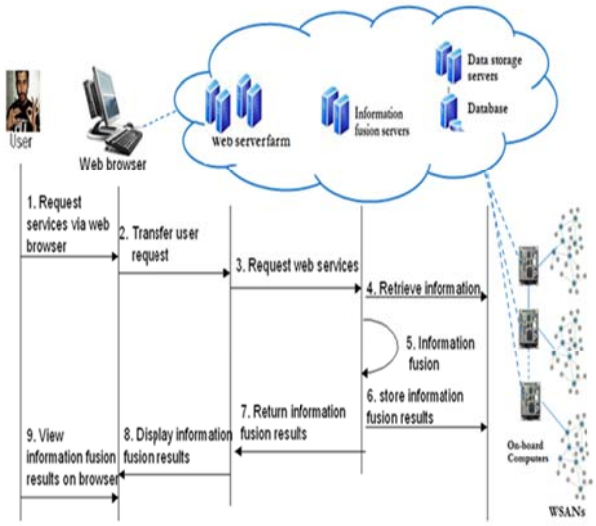

Figure 2: Web information management sequence

grid and deliver, autonomous services to various user applications. As Infrastructure software will expand to incorporate multi-sensor/actuator feeds such systems are subject to severe bandwidth loading and potentially may require large amounts of computing power and storage. As we move to consider broader multi-sensor/actuator installations, these limitations might be

further exacerbated. Biology inspired, alternative approach would be able to dramatically reduce the bandwidth, computing and storage requirements while allowing multi-sensor/actuator information and control to be shared between many diverse infrastructure software solutions. The human body is an excellent example of a true multi-sensor/actuator system being used for a multitude of diverse infrastructure software. As can be seen in the Fig. 3, much of the bodies data is being constantly processed by the brain at the *Unconscious* and the *Semiconscious* levels in the background without the direct involvement of the reasoning or cognitive part of the brain. In this way, the brain is capable to obtain information from the Semiconscious parts, when required and then integrate, via data/ctrl AI, with the *Conscious* world. If the human brain was not compartmentalised in this specific manner, the *Conscious* part of the brain would be completely overloaded with just trying to process the data or events required for the control of *Unconscious* body functions such as respiration, blood circulation, heart rate, temperature control not to mention immune, endocrine or cutaneous system functions. The only time that this Unconscious world communicates with the *Conscious* part of the brain is when serious anomalies are detected, i.e. a high temperature or low sugar levels is signalled to the *Conscious* world where reasoning then takes place followed by *Conscious* actions - take a pill, eat, call the doctor etc.

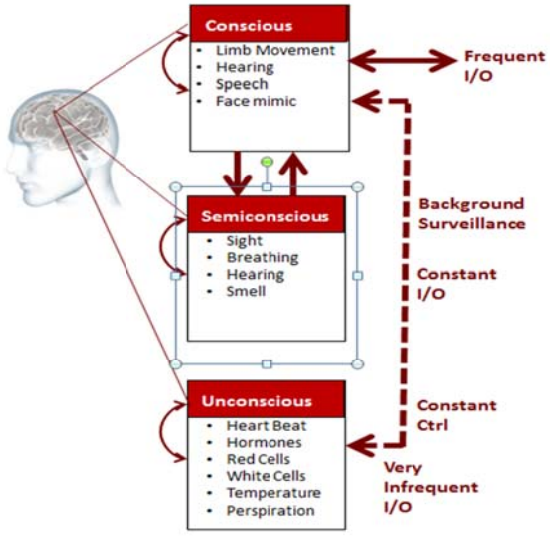

Figure 3: A model of IoT with autonomic feedback & Data/Ctrl

However, the breakdown of computing and communication for optimal data/ctrl AI is a non-trivial problem. The fundamental question is: what processing or control should be executed at the sensor/actuator level, if it has some computing power and what needs to be done at the intelligent controller (Linux box) level; And ultimately what computations need to be carried out at the ambient management level (application layer). One of the suggested approaches might be to first break down the information AI problem in terms of its distribution of communication and computing load in a highly flexible manner and then mapping the information AI on to the proposed architecture. It is proposed to use the emerging IEEE 1451 TEDS standards for effective discovery and maintenance methodologies of transducer (sensor and actuator) infrastructure.

4.3. Software tools and technologies for IoT

Wireless sensors, actuators, various computing devices and technologies play a critical role in the infrastructure (Fig. 4) of IoT base solutions. Advanced software development tools are not only to enable rapid modelling, design, implementation and integration of infrastructure oriented software but also to facilitate transaction processing, manage demands for computing resources, support flexible software composition, provide data from all sensors for the comprehensive assessment of processing conditions and allow software constructs which can support combination of real-time decisions or perceptions from multiple sources. With the advent of wireless sensor and actuators, MEM devices, application developers need to be in a better position to overcome the traditionally over-conservative, less-transparent, labour intensive and costly approach in terms of design development and maintenance of software.

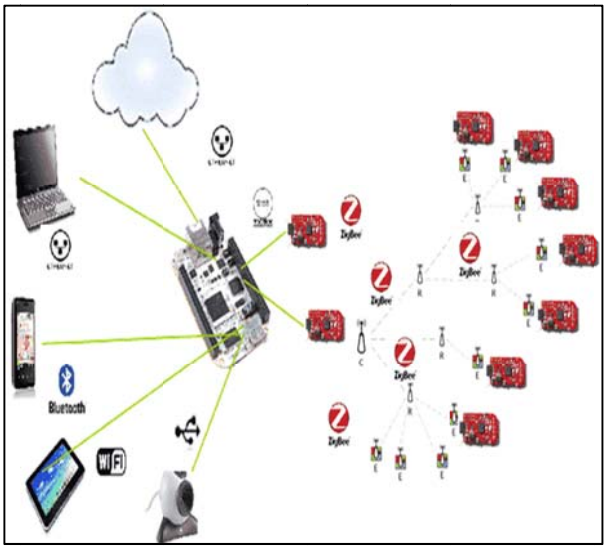

Figure 4: Wireless sensors and actuators technology in a prototype of IoT system

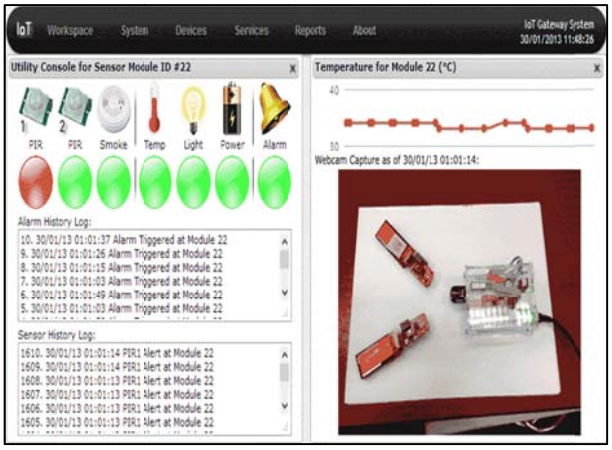

Figure 5: Rapid modelling, design, implementation using open source IoT hardware and software tools.

5. DISCUSSION

There are several challenges that modelling of the autonomic monitoring and control functions for IoT systems need to address. These challenges related to such important questions as:

How much intelligence needs to be local and how much can be group intelligence?

It is expected that group intelligence would bring certain tangible benefits. However each individual intelligent mote should have sufficient competence to complete a limited number of tasks on its own taking into account the special, and non-trivial, situation of autonomous execution of various tasks. It is considered that the interplay of these complimentary goals will be beneficial to the development process.

How to design intelligent behaviour (cooperation) in the IoT collective?

It is suggested that three classical rules (Reynolds 1987) should be followed:

1. Separation: do not move too close to nearby members of the collective (drones),
2. Alignment: move into the general direction of the collective (swarm) , and
3. Cohesion: steer towards the general centre of the collective.

It would be interesting to explore automated survival schema that run on MCU's for the situation where the CPU has failed and a limited set of MCU's remain to recover the vehicle. Some evolutionary algorithms for generating and prioritizing scenarios that are subsequently installed on MCU's to provide an adaptive way of fine tuning these schema. It would be possible and that it may even be possible to place adaptive seeds on an MCU allowing them to be somewhat adaptive once the CPU has failed and a vehicle wishes to return to a safe haven.

Other ideas related to cooperation within a swarm may involve exploration of decay properties of pheromone-like or hormone-like (endocrine system) paradigms that could involve encapsulation of weighting system which could allow some more subtlety of control. The decaying positional marker is stigmergy information left by some individuals of a given species for other members of the same species that could be accessed or modified when they come close or pass that point. An information token, or a tuple of information could encapsulate anything, including relations or behaviour of the vehicle (function/computation components). In addition to varying in the time domain through a timed decay, we can modify the relevant information for the individual drone/swarm in the light of changing external conditions to share with the new or old arrivals various information including the relative time sequence or even provide some serendipitous data/info for future use. Additionally, even computational components (whole algorithms) not only some proven parameters or artefacts i.e. images, sounds, graphs, text, etc. can be shared or exchanged. These shared elements can be used to environmental monitoring and forecasting as well as can be used for the decision making in IoT collective of various network and robotic devices.

6. CONCLUSION

The discussed modelling and simulation approaches involve the cutting edge technology of software infrastructure, technologies as well as application of heuristic (AI) techniques in IoT based systems. IoT systems, can be highly dependent on tight coupling between the user applications, infrastructure oriented software, the AI solutions, on-board computer(s). At the low level, IoT system relies on a large number of sensors and actuators devices which might be difficult to deploy and manage. Additionally, the autonomic management paradigm may be limited by actuating and sensing capability of proprietary technologies and devices in IoT systems. Collective intelligence and communication in IoT brings in a new set of challenges and complexities that can be addressed using bio-inspired ambient computational models as well as open hardware/software solutions.

REFERENCES

Bruzzone, A.G., Longo, F., 2005. Modeling & Simulation applied to Security Systems. *Proceedings of Summer Computer Simulation Conference*, pp. 183-188. July 24-28, Philadelphia (Pennsylvania, USA).

Reynolds, C.W., 1987. "Flocks, herds and schools: A distributed behavioral model". *Computer Graphics* **21** (4): 25–34.

Bak, P., 1996. *How Nature Works: The Science of Self-Organized Criticality*. Springer Verlag, New York.

Bejan A., 2002. Constructal Theory of Organization in Nature: Dendritic Flows, Allometric Laws and Flight", *Design and Nature*, Edited by: C.A. Brebbia & L.J. Sucharov, Wessex Institute of Technology, UK and P. Pascolo, Universita degli

di Udine, Italy, Transactio**n:** *Ecology and the Environment* vol. 57.

Bonabeau, E., Dorigo, M. and Theraulaz, G., 1999. Swarm Intelligence: From Natural to Artificial Systems, Oxford University Press,

Calder, W.A., 1984. Size, function and life history. Harvard University Press, Cambridge, Mass.

Chaczko, Z. (2007) Autopoietics of Biomimetic Middleware System, private correspondence, November.

Darveau, C. A., Suarez, R. K., Andrews, R. D., & Hochachka, P. W. 2002. Allometric cascade as a unifying principle of body mass effects on metabolism, *Nature*, 417:166-170.

Das, S. K. , Banerjee, N. and Roy, A., 2004. Solving Optimization Problems in Wireless Networks using Genetic Algorithms, Handbook of Bioinspired Algorithms.

Ishida, Y., 1997. The immune system as a prototype of autonomous decentralized systems: an overview," *In proceedings of 3rd International Symposium on Autonomous Decentralized Systems* (ISADS 97).

Kaiser, C., Kröckel, J. and Bodendorf, F., 2010. Swarm Intelligence for Analyzing Opinions in Online Communities. Proceedings of the 43rd Hawaii International Conference on System Sciences, pp. 1–9.

Kaufmann, S.A., 1995. At Home in the Universe: The Search for the Laws of Self-Organization and Complexity. Oxford University Press, New York.

Kennedy, J., 2006. Swarm Intelligence, in *Handbook of Nature-Inspired & Innovative Computing*, Editor: A. Zomaya, Springer Verlag, New York, pp.187-221.

Loureiro, A.A.F. and Ruiz, L.B., 2007. Autonomic Wireless Networks in Smart Environments, In Proceedings of the 5th Annual Conference on Communication Networks and Services Research, CNSR '07. Fredericton, New Brunswick, Canada.

McMahon, T. A. and Bonner, J. T., 1983. On Size and Life. Scientific American.

Niklas, K. J. 1994. Plant allometry: The scaling of form and process. University of Chicago Press, Chicago.

Phillips M.L., 2006. "Study challenges metabolic scaling law," *The Scientist*, January 26. http://www.the-scientist.com/news/display/23012/

Brown, P., Lauder, H., 2000. "Collective intelligence". In S. Baron, J. Field & T Schuller. *Social Capital: Critical Perspectives*. New York: Oxford University Press.

Noubel, J-F, 2004. "Collective Intelligence: the Invisible Revolution", rev. 2007.

Por, George (1995). "The Quest for Collective intelligence". In K. Gozdz. *Community Building: Renewing Spirit and Learning in Business*. San Francisco: New Leaders Press.