Chapter 2.23
Towards Autonomic Infrastructures via Mobile Agents and Active Networks

Stamatis Karnouskos
SAP Research, Germany

ABSTRACT

As we move towards service-oriented complex infrastructures, what is needed, security, robustness, and intelligence distributed within the network. Modern systems are too complicated to be centrally administered; therefore, the need for approaches that provide autonomic characteristics and are able to be self-sustained is evident. We present here one approach towards this goal, i.e., how we can build dynamic infrastructures based on mobile agents (MA) and active networks (AN). Both concepts share common ground at the architectural level, which makes it interesting to use a mix of them to provide a more sophisticated framework for building dynamic systems. We argue that by using this combination, more autonomous systems can be built that can effectively possess at least at some level of self-* features, such as self-management, self-healing, etc., which, in conjunction with cooperation capabilities, will lead to the deployment of dynamic infrastructures that autonomously identify and adapt to external/internal events. As an example, the implementation of an autonomous network-based security service is analyzed, which proves that denial of service attacks can be managed by the network itself intelligently and in an autonomic fashion.

INTRODUCTION

Systems and services are becoming more ubiquitous, which calls for sophisticated solutions to be in place. As we move towards the "Internet of things" (Dolin, 2006), it can be expected that millions of devices of different size and capability will be connected and interact with each other

over IP, e.g., sensor networks (Marsh, 2004). Therefore, any approach will have to take into consideration that:

- Complexity will increase
- Heterogeneity in devices, software platforms, online services, etc., will increase
- A large proportion of end-nodes will be connected wirelessly to the backbone infrastructure (the line of wired vs. wireless systems will blur more)
- Bandwidth and computing power will increase
- Ad-hoc computing, collaboration, task delegation, and environmental adaptation will be basic necessities
- On-demand software and service deployment will be vital
- Security and its satellite services will gain importance

In such an assumed future infrastructure, autonomic systems are expected to be of considerable help, since they will be able to be at a great degree self-sustained and also react to a dynamic changing environment.

Autonomic computing (Sterritt et Al., 2005) was introduced by IBM as a means to target increasing computer system complexity, and aimed initially at automating management of enterprise computational systems. In *The Vision of Autonomic Computing* (Kephart & Chess, 2003) it is stated that the dream of interconnectivity of computing systems and devices could become the "nightmare of pervasive computing," in which architects are unable to anticipate, design, and maintain the complexity of interactions. The essence of autonomic computing is system self-management, freeing administrators from low-level task management whilst delivering an optimized system. In a self-managing system, or Autonomic System, the human operator does not control the system directly, but only defines general policies and rules that serve as an input for the self-management process. For this process, IBM has defined the following four functional areas:

- **Self-configuration:** Automatic configuration of components
- **Self-healing:** Automatic discovery, and correction of faults
- **Self-optimization:** Automatic monitoring and control of resources to ensure the optimal functioning with respect to the defined requirements
- **Self-protection:** Proactive identification and protection from arbitrary attacks

There are two strategies in achieving autonomic behavior, i.e., through adaptive learning and via integral engineering into systems (Sterritt, 2004). Our approach focuses on how to engineer such an autonomous system, while adaptive learning, or self-learning, is seen as an ad-hoc component that can be imported from the domain of intelligent agents.

AMALGAMATION OF ACTIVE NETWORKS AND MOBILE AGENTS

Active and programmable networks (Karnouskos & Denazis, 2004) introduce a new network paradigm where network-aware applications and services can be not only distributed, but also can configure the heterogeneous network to optimally respond to task-specific requirements. We are able to utilize within the network: (a) computation, as we are able to compute on data received from active nodes, and (b) programmability, as we can inject user code into the network nodes in order to realize customized computation. Being able to achieve the above, we succeed in decoupling network services from the underlying hardware, deploy fine-grained customized services, relax the dependencies on network vendors and