Autonomic Management of Mobile and Wireless Networks

Antonis M. Hadjiantonis

KIOS Research Center for Intelligent Systems and Networks, University of Cyprus
antonish@ucy.ac.cy

Abstract. Autonomic management is receiving intense interest from academia and industry, aiming to simplify and automate network management operations. Autonomic management or self-management capabilities aim to vanish inside devices, relieving both managers and users from tedious configuration and troubleshooting procedures. Ideally, self-managed devices integrate self-configuration, self-optimization, self-protection and self-healing capabilities. When combined, these capabilities can lead to adaptive and ultimately self-maintained autonomic systems.

Keywords: autonomics, policy-based, self-management, network management.

1 Introduction

Mobile and wireless networks have become a ubiquitous reality and evermore surround our everyday activities. They form and disappear spontaneously around us and have become new means for productivity and social interaction. Access to corporate networks, e-mail or simply entertainment, these are the new necessities posed on an increasingly networked wireless world. In the era of mobility and connectivity, a multitude of devices interact with us in our everyday life. Wireless digital assistants such as mobile phones, laptops or personal organizers must be able to cope and offer the desired services at any place and at anytime. An increasingly ad hoc element facilitates the need for on demand connectivity and wireless communication. At the same time, increased complexity and heterogeneity have become barriers to seamless integration and ease of use.

In reality though, the deployment of self-managed networks is withheld from several obstacles that need to be overcome in order to realize such a vision. The use of policies for network and systems management is viewed as a promising paradigm to facilitate self-management. Policies can capture the high-level management objectives and can be automatically enforced to devices, simplifying and automating compound and time-consuming management tasks.

Nowadays, services targeting home and business users, such as Internet access, digital television or online entertainment, are taken for granted. However, modern lifestyle creates the need for extending the reach of such services but also creates the need for new ones, targeted to people on the move. The convergence of fixed and

A.M. Hadjiantonis and B. Stiller (Eds.): Telecommunication Economics, LNCS 7216, pp. 199–208, 2012.

wireless technologies is inevitable and a rapidly evolving market brings new challenges. In recent years, we have experienced an unprecedented penetration of mobile phones, while the mobile industry growth and evolution continues steadily. Developed countries are planning their transition to fully converged networks and services, while wireless access capability (Wi-Fi) is becoming a common feature of mobile phones. At the same time, newly industrialized countries and emerging markets are just discovering wireless technologies and offer an impressive drive for low cost infrastructure development. Their massive potential customer base is contrasted to low population density, making the cost of wired technologies prohibitive and deeming current management paradigms as inapplicable. At the same time, new wireless networking and management paradigms are investigated, offering a promising and challenging ground for research and innovation.

Improved network organization can increase scalability and decentralize management responsibilities, but one has to consider that the majority of wireless networked devices are not under the strict control of a network operator as in traditional infrastructure-based networks. Therefore, a critical management requirement is to respect the owner relationship between end-users and managed devices. Individual users are reluctant to entrust the command of their devices to an operator and demand more control. The lack of a single administrative authority complicates management tasks, but at the same time motivates research on collaborative management schemes. Open standards and contractual agreements can facilitate the interests of different managing entities, e.g. network operators or service providers. The goal is to provide an adaptive framework for network and service management, where users' privacy and preferences are respected, while multiple managing entities can offer services tailored to the users' needs.

The policy-based management (PBM) paradigm can provide the means to integrate self-management capabilities and policies can capture the high-level management objectives to be autonomously enforced to devices. Although the PBM paradigm has been traditionally employed in large-scale fixed IP networks, its controlled programmability can significantly benefit the highly dynamic environment of mobile and wireless networks. PBM can offer a balanced solution between the strict hard-wired management logic of current management frameworks and the unrestricted migration of mobile code offered from mobile agents. This has motivated the adoption of PBM for the autonomic management of mobile and wireless networks, aiming to simplify and automate compound time-consuming management tasks. The centralized orientation of policy-based operations requires significant research efforts to accommodate the needs of distributed policy-based management (D-PBM) for the next generation of mobile and wireless networks. In addition, in a rapidly evolving multi-player environment, policies can express the interests of different players and facilitate their cooperation. PBM can be a future-proof solution and can provide the flexibility to adapt to change. At the same time, the users' requirements for control and privacy can be encapsulated in policies and with minimum intervention their devices can operate autonomously.

2 Policy-Based Management (PBM)

Policy-Based Management (PBM) [2][15][13] and policies have been envisioned as encapsulating business objectives which in turn are autonomously applied to managed systems, requiring minimal human intervention. However, practice has shown that what was initially conceived as the instant panacea of network management is in fact a long journey towards self-managing networks, hampered by severe obstacles. The views published in [4] by a major infrastructure vendor are illustrative of initially overestimated expectations from policies: “to many people, it suggests that, by some magic, you get something for nothing, or at least without needing to think through what needs to be precisely done to achieve those objectives. Of course, there is no magic, and anyone expecting magic is bound to be disappointed”. Beyond initially high expectations, research on PBM has gradually verified its enormous potential and showed that it can simplify complex management tasks of large-scale systems. The concept of high-level policies monitoring the network and automatically enforcing appropriate actions has received intense interest and has been fuelled by the renewed interest in Self-Management and Autonomic Networking [2][15][13].

In general, policies can be defined as Event-Condition-Action (ECA) clauses, where on event(s) E, if condition(s) C is true, then action(s) A is executed. Different definitions and classification of policies can also be found in the literature and are presented later. The main advantage which makes a policy-based system attractive is the functionality to add controlled programmability to the managed system, without compromising its overall security and integrity [5]. Real time adaptability of the system can be mostly automated and simplified by the introduction of the PBM paradigm. According to [5] policies can be viewed as the means to extend the functionality of a system dynamically and in real time in combination with its pre-existing hard-wired management logic. Policies offer the unique functionality to the management system of being re-programmable and adaptable, based on the supported general policy types. Policies can be introduced to the system and parameterized in real time, based on management goals and contextual information. Policy decisions prescribe appropriate actions on the fly, to realize and enforce those goals.

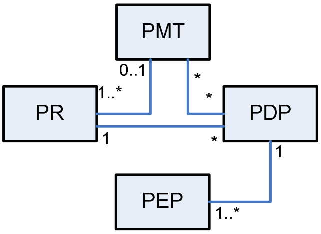

Fig. 1. PBM functional elements

A block diagram of PBM functional elements is shown in Figure 1, using a simplified UML notation of their relationships. These four elements constitute IETF’s policy-based framework, as proposed through the work of the Policy Framework WG (POLICY) and the Resource Allocation Protocol WG (RAP):

- Policy Management Tool (PMT): the interface between the human manager (e.g. a consultant or network administrator) and the underlying PBM system.
- Policy Repository (PR): the blueprint of policies that a PBM system is complying with at any given moment. It encapsulates operational parameters of the network and therefore it is one of the most critical elements.
- Policy Decision Point (PDP): a logical entity that makes policy decisions for itself or for other network elements requesting such decisions. These decisions involve on one hand evaluations of policy rule conditions and on the other hand deal with the actions' enforcement when conditions are met.
- Policy Enforcement Point (PEP): a logical entity that enforces policy decisions. Traditionally, the sole task of PEP is to execute policy decisions, as instructed by the controlling PDP.

The IETF framework is widely used and accepted in research and industry and has served as a reference model for PBM systems [16],[2]. Managing Entities use a Policy Management Tool (PMT) to introduce and store policies in the Policy Repository (PR). The PR is a vital part for every policy-based system because it encapsulates the management logic to be enforced on all networked entities. Stored policies can be subsequently retrieved, either by Policy Decision Points (PDP) or by another PMT. Once relevant policies have been retrieved by a PDP, they are interpreted and the PDP in turn provisions any decisions or actions to the controlled Policy Enforcement Points (PEP).

Policy provisioning is the process of communicating policy decisions and directives between a Policy Decision Point (PDP) and a Policy Execution Point (PEP) using a suitable protocol (RFC2753, RFC3198). A PDP is also known as a policy server, reflecting its responsibility to serve a number of PEP with policy decisions and relevant PBM information. On the other hand, PEP are also known as policy clients since their operation depends on these decisions, as provided by their parent PDP. The protocol involved in this communication is the policy provisioning protocol. Efforts from IETF's Resource Allocation Protocol Working Group (RAP WG) have produced the COPS (Common Open Policy Service) Protocol (RFC2748) and COPS protocol for Policy Provisioning (COPS-PR) (RFC3084). COPS is a simple query and response protocol that can be used to exchange policy information between a policy server (PDP) and its clients (PEP). The basic model of interaction between a policy server and its clients is compatible with IETF's policy-based framework. The focus of IETF's efforts has been mainly to provide a protocol to carry out the task of policy provisioning mostly related to QoS parameters and setup. Beyond COPS, no other dedicated policy provisioning protocol has been standardized by the IETF and policy provisioning has been viewed under the general umbrella of configuration management protocols. Traditional management protocols (SNMP) and interfaces (command line interface) are in use to carry out policy provisioning in an application-dependent manner. PBM frameworks based on Java (e.g., Ponder) have used RMI (Remote Method Invocation) to carry out provisioning. However, having in mind their deficiencies [10] and the need for interoperable standards, research community and industry have been moving toward XML-based management protocols. The trend towards Web Services and XML/HTTP-based management has also affected PBM.

3 Self-management and the Autonomic Paradigm

Self-management refers to the ability of independently achieving seamless operation and maintenance by being aware of the surrounding environment [6]. It has been closely related with autonomic computing and self-maintained systems [8]. This ability is widely embedded in the natural world, allowing living organisms to effortlessly adapt to diverse habitats. Without planning or consciousness, body's mechanisms work in the background to maintain a constant temperature. To imitate nature's self-managing abilities and apply them to the management of network and systems, the latter should be provided with the logic and directives for their operation and in addition the means to sense their operating environment. Self-management has been closely related with control systems and particularly to closed-loop controllers. By using a system's output as feedback, a feedback loop allows the system to become more stable and adapt its actions to achieve desired output. From the definitions above, it is evident that two main functions are required to support self-management. These two functions are interrelated and interdependent, thus forming a closed control loop with feedback (Fig. 2):

A. Provide the logic and directives to achieve seamless operation and maintenance.
B. Provide the means to sense and evaluate their operating surrounding environment.

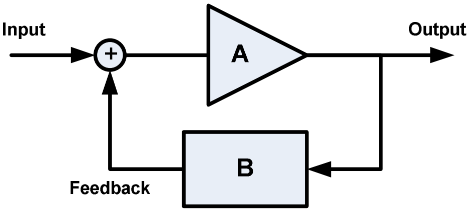

Fig. 2. Closed control loop with feedback

In 2001, an influential research declaration from IBM had introduced the concept of Autonomic Computing, which encapsulated the aspects of self-management in an architectural blueprint. The concept was inspired by the ability of the human nervous system to autonomously adapt its operation without our intervention and has appealed to researchers worldwide. IBM's vision [8] has fuelled intense research efforts both in industry and academia. In essence, autonomic computing and self-management are considered synonymous. According to IBM, "autonomic computing is a computing environment with the ability to manage itself and dynamically adapt to change in accordance with business policies and objectives." In addition, four quintessential properties of a self-management system were identified, frequently referred as self-* or self-CHOP properties:

- Self-Configuration
- Self-Healing
- Self-Optimization
- Self-Protection

Self-management concepts are increasingly used in research following the introduction of the autonomic manager (AM) component, as proposed by IBM. Major IT and Telco players are showing their research interest in autonomic networking and self-management, e.g. Motorola in [14] and Microsoft in [9] . In addition, intense interest is shown in autonomic network management from Academia [11]. The autonomic manager architectural component has become the reference model for autonomic and self-managing systems. It is a component that manages other software or hardware components using a control loop. The closed control loop is a repetitive sequence of tasks including Monitoring, Analyzing, Planning, and Executing functions. The orchestration of these functions is enabled by accessing a shared Knowledge base. The reference model is frequently referred as K-MAPE or simply MAPE, from the initials of the functions it performs. The use of a feedback loop raises concerns about a system's stability and according to control theory, a "valid operating region" of a feedback loop should be specified, indicating the range of control inputs where the feedback loop is known to work well [9]. Based on the definition of autonomic management, policies are identified as the basis of self-managing systems, encapsulating high-level business objectives.

Research on autonomic systems has been intense during the past years, aiming to embed the highly desirable self-managing properties to existing and future networks. The roadmap to autonomic management is indicative of a gradual evolution and can be used to evaluate a system's progress. Accordingly, management frameworks can advance through different maturity phases before becoming autonomic:

- Basic: manually operated management operations
- Managed: management technologies used to collect and synthesize information
- Predictive: correlation among management technologies provides the ability to recognize patterns, predict optimal configuration and suggest solutions to administrators
- Adaptive: management framework can automatically take actions based on available knowledge, subject to the supervision of administrators
- Autonomic: business policies and objectives govern infrastructure operation. Users interact with the autonomic technology tools to monitor business processes and/or alter the objectives

Apparently the road to self-management is long and a series of issues will need to be resolved on the way. Until now, a complete self-management solution is not available. Instead, researchers and practitioners have attempted to partially tackle self-management by implementing some of the desired properties and adopting a gradual transition. Each of the four desired capabilities is contributing to the overall goal of enabling truly self-managed systems.

4 Distributed Policy-Based Management for Mobile and Wireless Networks

The principles of autonomic management and self-organization are envisioned by researchers as a natural path for the Future Internet. Autonomic management is expected to simplify the painstaking tasks of managing complex large-scale systems through the use of automated closed-loop management. Therefore, rather than proposing a holistic framework for the Future Internet, the proposed approach concentrates on the design of those architectural entities that would facilitate autonomic wireless networking. Following an evolutionary path, each autonomic support entity (ASE) is designed as an extension of the ongoing Future Internet design, maintaining backward compatibility with today's Internet. Based on open standards and interfaces, this approach should ensure the interoperable and future-proof integration of ASEs with the evolving design of the FI.

Three cooperating autonomic support entities (ASE) are proposed for the enhancement of wireless and mobile networking in the FI:

1. Decentralization (DCN.ASE)
2. Mobility (MOB.ASE)
3. Ad hoc communications (AHC.ASE)

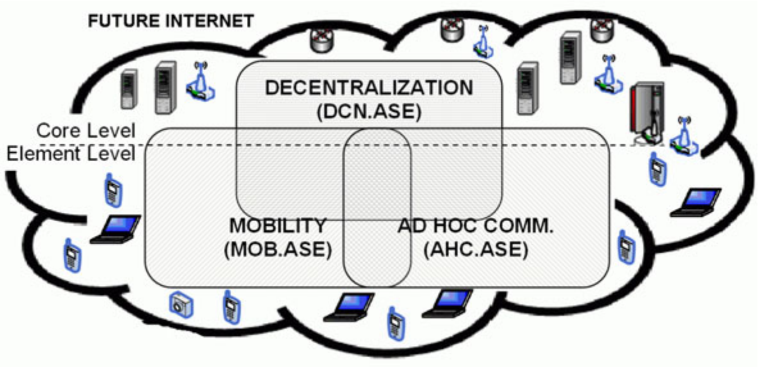

Fig. 3. Autonomic Support Entities for the Future Internet

As shown visually in Figure 3, these entities will operate and cooperate at different levels. They are designed address the lack of management decentralization (DCN.ASE), seamless mobility (MOB.ASE), and spontaneous communications (AHC.ASE) from today's Internet. The separation between Core and Element levels indicates the separation of functionality between the operator-owned network core and the user-owned devices respectively.

The motivation behind the Decentralization ASE is to enable collaborative management of large-scale networks, focusing on mobile and wireless access networks and their interconnection with fixed ones. A key goal is the efficient and scalable management of personal-area networks (PAN). In addition, the secure interactions of mobile and nomadic PANs with authorized or non-authorized wireless local-area networks (WLANs), as well as wide-area networks (WANs), will need to be addressed. The functionality of this entity is based on the distributed policy-based management (DPBM) paradigm and spans equally between core and element levels.

This means that part of the entity's functionality will be hosted in the network core, e.g. policy definition, conflict resolution and business plan implementation. However, an important part will be hosted on network elements, i.e. devices owned by end-users. Such functionality will include policy distribution, local management activities, user preference enforcement and privacy protection. For the latter end-user functionality, the Decentralization ASE will cooperate with the Mobility and Ad hoc communication ASEs, provisioning them with the appropriate policies that guide their autonomic behavior. The Mobility ASE will enable the seamless connectivity of users between different access networks and different devices as well, while the Ad Hoc Communications ASE will cater for the users' need for spontaneous communications. The cooperation of these entities is enabled though the Distributed PBM infrastructure (Figure 4), which decentralizes management tasks and pushes intelligence closer to the network edge. This can result in quicker reaction times and policy decisions for users, thus resulting in more stability. For more details on the implementation and evaluation of DPBM, the reader is referred to [7] and references within.

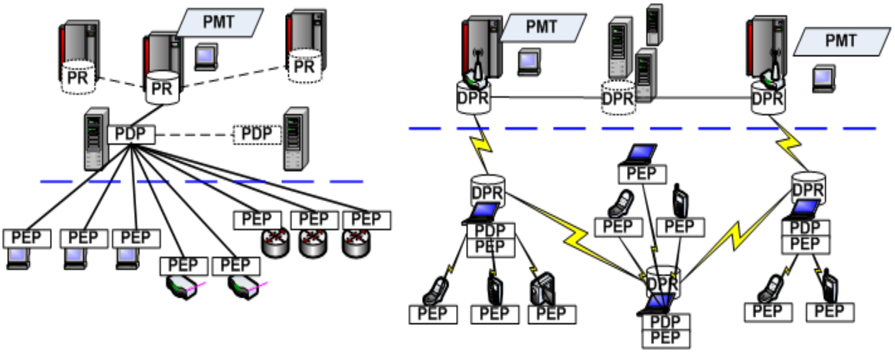

Fig. 4. Centralized versus Distributed PBM

5 Open Issues

While autonomic management is gradually implemented in today's networks, there are several open issues that need to be resolved. We focus on the two most prominent, indicating the scope for further examination and future work.

- Centralized vs. distributed control: the architecture of PBM systems is predominantly based on a centralized or hierarchical paradigm, following the organization of the managed networks. As a result, the majority of PBM functionality and protocols follow these paradigms, e.g. the manager-agent model for policy provisioning and the centralized policy repository storage. To enable distributed PBM, the coordination of multiple policy decision points (PDP) needs to be addressed in combination with decentralized policy storage and provisioning. Recently, the emergence of highly distributed computing systems (cloud computing) has motivated the decentralization of policies and their distributed management. Departing from centralized PDPs deployment, the distributed control of multiple PDPs need to be investigated.

- Conflicting policies and policy analysis: policy refinement is the process of deriving a concrete policy specification from higher-level objectives or goals [12]. It is an important process that leverages the potential of PBM frameworks, therefore it has received significant research interest, aiming to provide automated solutions [1]. The process is further hampered by the risk of producing inconsistent policy specifications, giving rise to concerns about policy conflicts and the need for policy analysis. The need for policy analysis and the lack of tested solutions is one of the main drawbacks of policy-based systems. Policy analysis [3] refers to the examination of policies and the verification of their current and future consistency. In complex environments where a number of policies need to coexist, there is always the likelihood that policies may conflict, either because of a specification error or because of application-specific constraints. It is therefore important to provide the means of detecting conflicts in the policy specification.

In spite of obstacles, the benefits from implementing autonomic and policy-based management solutions are significant. The industrial interest in standardization activities of 3GPP, like Self-Organizing Networks (SON) [18],[19] and Policy Charging and Control (PCC) [17] architecture, illustrate the potential of the described concepts and open new avenues for R&D.

Acknowledgements. This work is supported by the Cyprus Research Promotion Foundation's Framework Program for Research, Technological Development and Innovation 2009-2010 (DESMI 2009-2010), co-funded by the Republic of Cyprus and the European Regional Development Fund, and specifically under Grant ΔΙΔΑΚΤΩΡ/0609/21.

References

1. Bandara, A.K., et al.: Policy refinement for IP differentiated services Quality of Service management. IEEE Transactions on Network and Service Management 3(2), 2–13 (2006)
2. Boutaba, R., Aib, I.: Policy-based Management: A Historical Perspective. J. Netw. Syst. Manage. 15(4), 447–480 (2007)
3. Charalambides, M., et al.: Dynamic Policy Analysis and Conflict Resolution for DiffServ Quality of Service Management. In: 10th IEEE/IFIP Network Operations and Management Symposium, NOMS 2006, pp. 294–304. IEEE (2006)
4. Clemm, A.: Network Management Fundamentals. Cisco Press (2006)
5. Flegkas, P., Trimintzios, P., Pavlou, G.: A policy-based quality of service management system for IP DiffServ networks. IEEE Network 16(2), 50–56 (2002)
6. Hadjiantonis, A.M., Pavlou, G.: Policy-Based Self-Management in Wireless Networks. In: Context-Aware Computing and Self-Managing Systems, pp. 201–272. CRC Press (2009)

7. Hadjiantonis, A.M., Pavlou, G.: Policy-based self-management of wireless ad hoc networks. In: IFIP/IEEE International Symposium on Integrated Network Management, IM 2009, pp. 796–802 (2009)
8. Kephart, J.O., Chess, D.M.: The vision of autonomic computing. Computer 36(1), 41–50 (2003)
9. Mortier, R., Kiciman, E.: Autonomic network management: some pragmatic considerations. In: ACM Proc. 2006 SIGCOMM Workshop on Internet Network Management, INM 2006, Pisa, pp. 89–93 (2006)
10. Pavlou, G.: On the Evolution of Management Approaches, Frameworks and Protocols: A Historical Perspective. J. Netw. Syst. Manage. 15(4), 425–445 (2007)
11. Pavlou, G., Hadjiantonis, A.M., Malatras, A. (eds): D9.1:Frameworks and Approaches for Autonomic Management of Fixed QoS-enabled and Ad Hoc Networks. EMANICS Network of Excellence, Deliverable (2006), http://www.emanics.org
12. Sloman, M., Lupu, E.: Security and management policy specification. IEEE Network 16(2), 10–19 (2002)
13. Strassner, J.: Policy-Based Network Management: Solutions for the Next Generation. Morgan Kaufmann (2003)
14. Strassner, J., Raymer, D.: Implementing Next Generation Services Using Policy-Based Management and Autonomic Computing Principles. In: 10th IEEE/IFIP Network Operations and Management Symposium, NOMS 2006, pp. 1–15 (2006)
15. Verma, D.: Policy-Based Networking: Architecture and Algorithms. Sams (2000)
16. Verma, D.C.: Simplifying network administration using policy-based management. IEEE Network 16(2), 20–26 (2002)
17. 3GPP specification: 23.203 Policy and charging control architecture, http://www.3gpp.org/ftp/Specs/html-info/23203.htm
18. 3GPP specification: 32.500 Telecommunication management; Self-Organizing Networks (SON); Concepts and requirements, http://www.3gpp.org/ftp/Specs/html-info/32500.htm
19. 3GPP specification: 32.541 Telecommunication management; Self-Organizing Networks (SON); Self-healing concepts and requirements, http://www.3gpp.org/ftp/Specs/html-info/32541.htm