

Challenges for Federated, Autonomic Network Management in the Future Internet

Brendan Jennings*, Rob Brennan†, William Donnelly*, Simon N. Foley‡, Dave Lewis†,
Declan O’Sullivan†, John Strassner*, Sven van der Meer*

*Waterford Institute of Technology, Ireland

{bjennings, wdonnelly, jstrassner, vdmeer}@tssg.org

†Trinity College Dublin, Ireland

{rob.brennan, dave.lewis, declan.osullivan}@cs.tcd.ie

‡University College Cork, Ireland

s.n.foley@cs.ucc.ie

Abstract—Regardless of which networking protocols or technologies form the core of the Future Internet it is clear that the environment as a whole will need to support a very broad range of business and user interaction modes. In today’s Internet we observe the growing trend for services to be both provided and consumed by loosely coupled value networks of consumers, providers and combined consumer/providers. In this paper we argue that this trend has major implications for network management in the Future Internet. In particular, we discuss six research challenges that we believe need to be addressed by the network management community if the potential for the Future Internet to flexibly support value networks is to be realized.

I. INTRODUCTION

Regardless of whether the Future Internet evolves from the existing Internet architecture or emerges following a clean slate design, there is broad agreement that it must provide powerful, yet low-overhead, network management capabilities. Existing network management approaches are typically theoretically centered around centralized control of a (relatively) small number of managed entities within a single administrative domain, augmented with some well-defined, but limited, coordination across domains. However, in practice business and technological concerns fragment this centralized model and the number of managed entities is rising rapidly. Such approaches are already becoming untenable in increasingly complex, heterogeneous and interconnected networks and are therefore, we believe, not suited to the more open and flexible environments envisaged for the Future Internet.

In the current Internet there is a trend for services to be both provided and consumed by loosely coupled *value networks* of consumers, providers and combined consumer/providers. We expect that, as user demands and business models evolve, support for such value networks will become a central requirement for the Future Internet, regardless of the technological choices made in its realization. These value networks sharply contrast with traditional value chains that are relatively static and have well-defined, long-lasting commercial relationships. The exchange of resources and services is no longer restricted to well defined commercial contracts, as typical in value chains; instead, access to resources and services is often granted more freely and fluidly [1]. The expectation is that this will

improve the value received by the ultimate user and thereby render additional value in some form to the other members of the network. In value networks the benefits accrued by members are often less tangible than direct financial rewards and often materialize unpredictably and over longer time periods. Examples of such benefits may be customer loyalty, the trust of partners needed to share risk in future ventures, and access to knowledge.

A central issue is therefore how network management systems must be evolved to achieve the flexibility and adaptability required of the Future Internet to support value networks? One promising approach is that of the autonomic network management [2], [3] paradigm, which promises a much more flexible approach to network management that seeks to both allow systems to automatically adapt offered services or resources in response to user or environmental changes and to simultaneously reduce operational expenditure for network operators. However, work to date has focused on autonomic management in the context of single, well-defined network domains. Consequently, we run the risk that the stovepipe design of current Operational and Business Support Systems, due in large part to operators’ desire to incorporate best of breed functionality, will be replicated in the Future Internet. This would prohibit the sharing and reuse of common data, which results in operators being unable to effectively manage increasing business, system and operational complexity.

To address the requirement of the Future Internet to flexibly manage the provision of communications (and other) services across network boundaries and in the context of evolving value networks, we introduce the concept of *federated, autonomic management of communications services*. This envisions network management systems where both local network autonomy is assumed and directed towards mediated business goals that provide services which transcend legal and organizational boundaries in dynamic networks of consumers and providers. Such systems can be characterized as follows:

- *Federated* refers to the ability of such systems to enable network and service management for evolving value chains composed of providers and/or consumers;
- *Autonomic* reflects the ability of such systems to be aware

of both themselves and their environment, so that they can self-govern their behavior within the constraints of the business goals that they collectively seek to achieve;

- *Management* refers to the ability of such systems not just to configure, monitor and control a network element or service, but also administer the lifecycle aspects of that resource or service in a programmable way, empowering service quality of experience management by end-users themselves;
- *Communications Services*, refers to the requirement for such systems to focus on services provided in value networks, not on networks and network elements. The goal is to facilitate services being offered in a portable manner that is independent of the utilized networks.

In the paper we discuss the scientific challenges that we believe must be addressed by the network management community if federated, autonomic management for communications services is to be achievable in the Future Internet. These challenges are not all new – aspects of most of them have been actively researched by the network management community over a number of years. However, as we move towards the Future Internet, we believe that it will be crucial that they are addressed in a coordinated manner, so that flexible, comprehensive management solutions can be delivered. We discuss six challenges and attempt to outline some initial approaches that we believe could yield significant advances.

II. THE CHALLENGES

In the following sections we identify six scientific and technical challenges, each of which we argue must be addressed to realize the vision of federated autonomic management for communications services. Figure 1 depicts a Future Internet scenario in which services are delivered end-to-end in the context of value chains across interconnect enterprise, home area, access and core networks, both fixed and wireless. We envisage federation of networks and network management systems at three levels of abstraction. At the lowest level, termed network infrastructure coordinated self-management, management systems should support self-management by the resources in a given domain, but ensure that this self-managed behavior is coordinated across management boundaries. At the middle level, termed service monitoring and configuration, management systems should configure network resources in a manner consistent with business goals, but in a manner that is consistent with configuration activity in neighboring network domains participating in a value network. Finally, at the highest level, termed federated service management, management systems should semantically interoperate to support evolving value chains and the end-to-end delivery of services therein.

Based on these levels we group our challenges into three pairs. The highest level challenges, relating to federated service management, are:

- *Federated Meta-Management*; and
- *Federated Semantic Mapping*

The first requires techniques for management of the distribution and enforcement of management decision-making

authority in dynamically formed federations. This must be supported by solutions to the second challenge, which relates to development of semantic analysis techniques to facilitate sharing and understanding of network and management information.

The mid-level challenges, relating to service monitoring and configuration are:

- *End-to-End Service-Level Monitoring*; and
- *Business-Driven Network Configuration*

These address the management of end-to-end service delivery. This involves: configuring service and network resources in accordance with the policies of the federation of actors involved; providing intelligent feedback to progressively improve management policies as service usage and resource utilization change; and providing rich usage data to guide rapid service innovation.

The lower level challenges, relating to network infrastructure coordinated self-management are:

- *Reusable Self-Management*; and
- *Co-ordinated Self-Management*

These address self-management capabilities for the network infrastructure that can coordinate across different administrative domains and different network technologies to optimize end-to-end service delivery within business constraints set by management systems.

We now explore these challenges in greater detail.

A. Federated Meta-Management

In order to efficiently support short service life-cycles within dynamic federations of service providers and their customers, management systems must be able to dynamically negotiate and realize federations with other management systems and achieve an appropriate balance between satisfying local and federation wide goals. This will require major extensions to current approaches for expression of system goals, negotiation mechanisms and distributed security.

Hence, the federated meta-management challenge is development of approaches to model, communicate, negotiate, control and secure management authority in a dynamic federation to enable the coordinated configuration of networks for flexible end-to-end service provision. The difficulty in solving this problem, lies in the difficulty of modeling the differing nature of diverse management approaches. A given resource, service, or entire network and their administrators can be a part of multiple federations simultaneously. User needs, business goals, and changing environmental conditions may force that resource or service to join and leave federations frequently, possibly in an ad-hoc manner. Different priorities will be placed on the value of federation membership by different resources and services, as well as by the managers and/or managing systems of those resources and services. This will influence the degree to which actors may wish to exert their management authority at any one time, or to delegate it to other actors in the federation. For instance, a commercial service provider, though wishing to minimize management

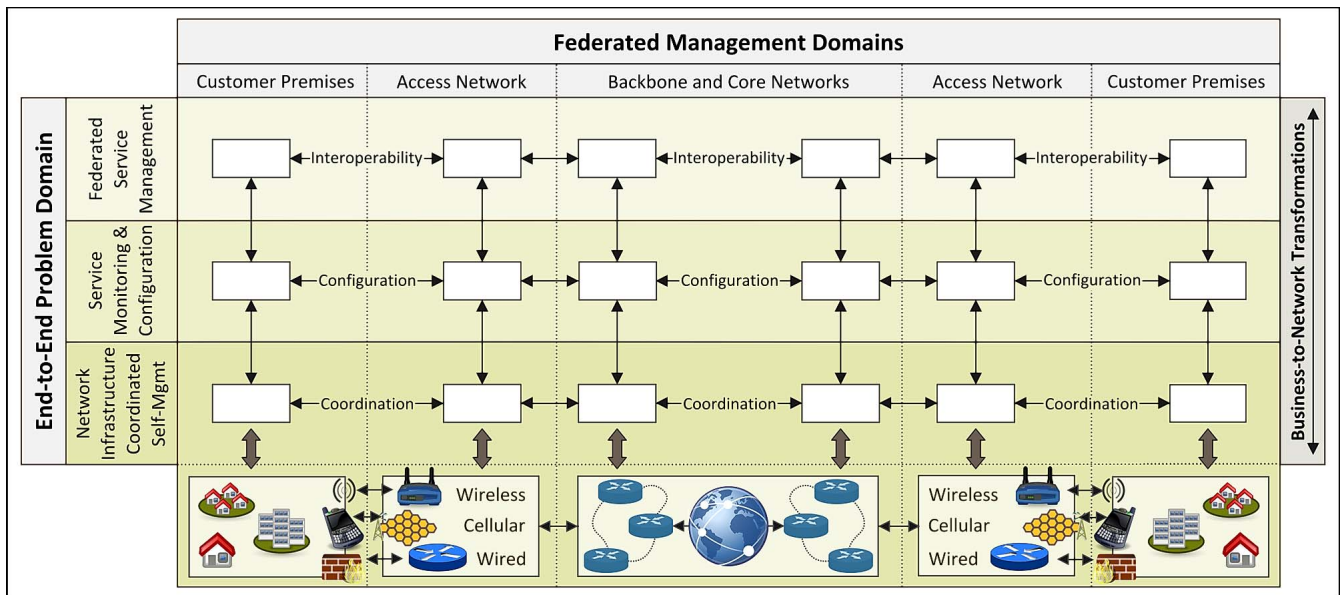


Fig. 1. Federated, Autonomic Management Domains for the Future Internet.

cost, may aim to exercise management authority to maximize its profitability.

1) *Potential Approaches*: Increased management flexibility and extensibility can be provided by Policy-Based Management (PBM) [4] and the semantic modeling of management information [2]. PBM is an increasingly popular method for combining flexibility with efficiency in systems and network administration [5], [6]. In PBM systems, administrators encode operational management decisions as rules, which are then mapped into concrete device configurations by the policy system. However, structural abstractions, such as roles [7] and domains [8], used in many policy rule languages, reflect hierarchical organizational thinking that have been shown to be insufficient for modeling the complex interrelationships between individuals within human organizations [9]. This results in the need for complex tools to manage changes to these policy rule languages which themselves become obstacles to interoperability and to change. Therefore, handling the authoring and maintenance of a coherent set of policies across a federation of providers presents significant problems for existing PBM systems with regards to policy conflict resolution and collaborative policy consensus forming. Recent advances in Community-Based Policy Management (CBPM) [10] have provided a model that is tailored such decentralized settings. However, understanding how progressive service management can be conducted using multiple CBPM systems, distributed over multiple service federations and customer value networks, in order to address this challenge requires further investigation. In particular, there are significant issues around how federations are formed, what level of trust are required to support this formation, and what patterns of decentralized authority would best support different forms of federations or value networks.

Considering trust in more detail, securing a federation presents a major issue, especially as service refinement and

innovation may spawn sub-federations of providers and customers. Again, in order to ensure that disparate policies are consistently enforced across federations, existing approaches (for example [11]) rely on centralized administrative authority. The Distributed Authorization Language (DAL) [12] has been designed specifically for decentralized coalition policies that do not require centralized authority. DAL-based security protocols supports dynamic coalition formation, coalition merging, and inter- and intra- coalition delegation while avoiding the delegation inconsistencies (subterfuge) that can arise [13] in conventional decentralized Trust Management systems. The key to avoiding subterfuge is the use of consistent policy knowledge which we argue could be achieved by adopting an ontology based approach. To address this, an integration of DAL into the CBPM scheme could be extended to support an ontology-based PBM.

B. Federated Semantic Mapping

Many problems in dynamically federating previously separated management domains will not be resolved simply by resolving rule (or policy) conflicts, because there is no underlying logic for resolving the conflict and, as importantly, verifying that the conflict has been resolved. Rather, such problems will require novel advances in semantic analysis, whereby heterogeneous representations of knowledge describing the state and behavior of managed resources can be harmonized and decisions enforced using unambiguous policy rules. The federated semantic mapping challenge is thus the development of mapping processes and techniques required to enable harmonization between heterogeneous semantic management models, e.g. embedded in contracts or policies, and to ascertain the extent to which these processes must be context-specific and amenable to automation.

1) *Potential Approaches*: The use of formal semantics, including mappings, in structured knowledge has already been demonstrated for autonomic communications approaches [14], [15]. Using these techniques it is possible to model: a) the resources being managed, b) the context used in communication services, and c) the policies used to express governance. For a federated environment, semantic mapping is essential to allow the sharing and common understanding of contracts and policies, which together govern the interactions between different management elements.

Traditional semantic mapping approaches, as surveyed in [16], generally assume that the mapping task is performed by a knowledge engineer, whose explicit task is to generate a full static mapping between models that will be used by several applications. Thus, the state of the art has a very constrained and static view of the semantic mapping process. By contrast, in federated autonomic communications management systems, the entities engaged will range from autonomic agents to operational managers and end users, requiring the development of a new methodology that can integrate disparate knowledge that is inherent to the autonomic environment. In addition, as argued in [17], mappings increasingly need to be generated to be task-specific, context-sensitive and able to represent partial knowledge. In addition, mappings will need to be tracked, managed and maintained over time, especially as source models for the mappings evolve. However, as yet there is little state of the art in annotating mappings with context and task specific information, or metadata that would allow for their ongoing management.

C. End-to-End Service-Level Monitoring

A key requirement for autonomic management systems is the ability to monitor their own environment so that they can react to changes and gather information to populate or specialize their own internal environmental models for planning and prediction. Since our proposed federation of autonomic systems acts to deliver end-to-end communication services, it is insufficient for individual federation members to monitor their own domains to guarantee properties of the end-to-end quality of experience. To close the federated, end-to-end autonomic control loop it is necessary to develop processes that provide service-level monitoring of the operational state of communications services across the boundaries of heterogeneous networks. The end-to-end service-level monitoring challenge is therefore the development of processes that can provide semantically rich service-level monitoring information relating to the operational state of the communications services across the boundaries of heterogeneous interconnected networks.

1) *Potential Approaches*: To address this challenge we believe it will be necessary to support both on-demand and continuous monitoring techniques that can be combined to (i) accurately identify the source of unexpected service degradation or other faults and (ii) support prevention of potential service degradation. Collected data will need to be shared across different administrative boundaries and processed in

a distributed, scalable manner that is conducive to analysis and contextualization using the aid of information or semantic models and reasoning techniques to ascertain the significance of individual monitored events in terms of their impact on the end-to-end delivery of services.

Monitoring data harmonization, as envisaged here, goes far beyond syntactical inter-working – it requires mechanisms for mapping and federation of the large volume of low level data produced by monitoring systems into semantically meaningful information and knowledge that may be discretely consumed by value network members. Any complex system has domain experts who are familiar with how the constituent parts of the system can be managed, and are particularly aware of the end-to-end operating constraints of those constituent parts. Encoding this expertise in a manner that can be utilized by other stakeholders is a difficult task [5], but one we believe can be solved through the application of knowledge representation and engineering techniques. The benefit of enabling such expertise to be encoded, aggregated and interpreted across diverse domains is that it will facilitate value network members monitoring other parts of the system and using this knowledge to inform management decisions made locally.

D. Business-Driven Network Configuration

The business-driven network configuration challenge is the development of processes that analyze monitoring information and use inferred knowledge to trigger policy management analysis and decision processes that result in the generation and deployment of a set of device configurations that best align a network's behavior with business goals. Current network management systems are significantly impaired by their inability to automate the translation of business information to network device configuration commands. Automating the translation of business level policies (specified in terms of entities such as products, services and customers) through a number of levels of abstraction into corresponding device instance level policies (configuration commands specified in terms of entities such as packet marking rules or firewall configuration rules) is hugely challenging, since information needs to be added (and removed) as the policies become more specific in nature.

1) *Potential Approaches*: We believe that the key to achieving business-driven network configuration is the maintenance within policy based management systems of a policy continuum [18], in which policies at different levels of abstraction are grouped in stratified business, system, network, device and device instance views mirroring the different constituencies of people that work together to define and deploy the policies that govern the delivery of products and services. Implementation of the policy continuum enables different constituencies, who understand different concepts and use different terminologies, manipulate sets of policy representations at a view appropriate to them, and to have those view-specific representations mapped to equivalent representations at views appropriate for manipulation by other constituencies. Policy authoring and analysis, including policy refinement, become significantly

more complex in the context of a policy continuum [18] and much research work needs to be done before systems implementing a policy continuum become deployable. One promising approach is to harness the expressive power of ontologies to detail the nature of the relationships between policy concepts at different levels of the continuum. Policy refinement processes can access this knowledge from the ontologies, and, applying ontological engineering techniques, propose candidate refinements, which in certain cases will need to be ratified by humans. Thus, we envisage policy refinement as a (semi-)automated process, where the level of human intervention decreases over time as the system learns from the outcome of previous refinements.

Policy refinement as described above relates to the identification of an appropriate set of device instance level configurations given changing business goals as manifested in newly authored (or modified) business level policies. However, changed business level policies are not the only trigger for reconfiguration of the network devices. Equally important is reconfiguration in the face of changing operational context of the network devices themselves. Based on information gathered by service-level monitoring processes such as those described in II.C it will be necessary to employ learning and reasoning techniques to analyze whether the systems actual state corresponds to the desired state (as indicated by currently deployed set of policies). In cases where it does not appropriate policy actions will be triggered which must then be refined to generate the appropriate new device configurations.

E. Reusable Self-Management

The Re-usable Self-Management challenge is the development of a suite of self-management algorithms and processes that can be re-used in a range of network types and that can be parameterized via policies to constrain their behavior in line with the business goals of the network operator. Currently proposed self-management algorithms and processes are typically tailored to one particular network type and cannot be readily adapted for use in other network types. Clearly no single routing algorithm can be applied, let alone result in optimal behavior across network types ranging from core networks to enterprise networks to wireless mesh and to various wireless access networks. However, it should be possible to develop a suite of self-management algorithms and processes that are applicable to different network types, but which are open to incorporation of specific sub-processes to address unique requirements (for example, distributed channel allocation in wireless access networks).

1) *Potential Approaches:* In developing these algorithms and processes, inspiration may be drawn from myriad sources, but in particular those mimicking self-management behavior exhibited by societal and biological systems have proven to be especially effective. Whilst similar proposals already exist in the literature with varying complexity and responsiveness profiles, a key issue is development of techniques that are appropriate for deployment in large-scale and heterogeneous network domains.

Whilst work on development of a suite of reusable decentralized self-management algorithms is crucial, deployment of these algorithms, whilst necessary, will not be sufficient. Equally important will be the flexible specification and enforcement of the goals these algorithms collectively seek to achieve goals designed to ensure that the network successfully delivers services to users. Thus, such processes should be designed so that their behavior can be readily constrained by management systems through policies that parameterize their operation. Results of initial work in this direction are reported by Balasubramaniam et al. [19].

F. Coordinated Self-Management

The coordinated self-management challenge is the development of algorithms and processes that coordinated their behavior, in accordance with constraints set by management systems, across heterogeneous networks to deliver effective end-to-end self-management. Much of the focus of current research in autonomic network management is on the development of highly distributed algorithms that seek to optimize one or more aspects of network operation and/or performance, in essence aiming to provide various self-management capabilities. The belief is that deployment of these capabilities will allow network operators manage their resources efficiently, with minimal human intervention, and at the same time, maximize both revenue and customer satisfaction.

Two key areas where self-management research may have a significant impact are resource management and adaptive inter domain routing. Whilst both areas have been extensively investigated, the majority of the work to date has concentrated on single network domains (either wired or wireless). However, when we consider that services must be delivered end-to-end across heterogeneous networks there would be significant benefits in designing self-management algorithms and processes that coordinate their behavior across network boundaries.

1) *Potential Approaches:* We envisage separate hierarchical processes that coordinate the self-management of individual networks in a manner such that adaptations of particular networks that affect neighboring networks will be stabilized in a timely manner. Development of such processes can profitably benefit from analysis of behavior exhibited by societal and biological systems. In the case of societal systems, behavior such as the symbiotic processes that allows individuals and communities to co-exist may be used to coordinate management processes across independently administered networks. In the case of biological systems, behavior such as the maintenance of equilibrium in the nervous or endocrine systems of the human body will be used to coordinate processes that ensure end-to-end network stability.

III. SUMMARY AND OUTLOOK

This paper discussed the main challenges facing the communication industry as it aims to tackle the dual goals of controlling operational support costs through autonomic systems and engineering those systems to be flexible enough to support

agile management decision making by service providers and their customers. Analogous to the way that the challenges were articulated in this paper around the needs of value networks, the industry must build on its strong history of R&D value networks to collectively address these challenges. Two current research-driven networks that are actively working to directly address federated, autonomic management systems are the Autonomic Communication Forum [20] and the Ireland-based FAME research cluster [21].

The Autonomic Communication Forum (ACF) is an international non-profit organization formed in 2006 with the aims of (1) unifying current thinking in autonomic communications by creating a new set of ACF sanctioned standards, focusing firstly on the management of systems, and secondly on computing and communications using autonomic mechanisms, (2) building on the above, defining an autonomic reference framework as well as a set of baseline compliance statements to guarantee interoperability, and (3) creating an organizational structure that will empower academia and industry to work together in developing and maintaining the above goals. The ACF is pursuing its aims through close coordination of academic researcher and industrial stakeholders, through a number of technical working groups, and through interactions with other standardization bodies and industry fora.

The FAME cluster, supported by Irish Government research funding was created in early 2009 to support academic-industrial collaboration to directly address the challenges laid out in this paper. This five year initiative will integrate academic research in this area with the involvement of the world leading multinational players in communications R&D, including Ericsson, Cisco, Alcatel-Lucent, IBM, Hewlett-Packard, and Telefónica I+D.

ACKNOWLEDGEMENT

This work was partly funded by Science Foundation Ireland via grant 08/SRC/I1403 ("Federated, Autonomic Management of End-to-End Communications Services").

REFERENCES

[1] V. Allee, *The Future of Knowledge: Increasing Prosperity through Value Networks*, Butterworth-Heinemann, 2003.

[2] B. Jennings et al., Towards Autonomic Management of Communications Networks, *IEEE Commun. Mag.*, vol. 45, no. 10, pp. 112-121, Oct. 2007.

[3] S. Dobson et al., A survey of autonomic communications," *ACM Trans. Auton. and Adapt. Syst.* vol. 1, no. 2, pp. 223-259, Dec. 2006.

[4] M. Sloman, Policy Driven Management for Distributed Systems, *J. Netw. Syst. Management*, vol. 2, no. 4, pp. 333-360, Dec. 1994.

[5] J. Strassner, *Policy-Based Network Management: Solution for the Next Generation*, Morgan Kaufmann, 2003.

[6] R. Boutaba, and I. Aib, Policy-based Management: A historical Perspective, *J. Netw. Syst. Management*, vol. 15, no. 4, pp. 447-480, Dec. 2007.

[7] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, Role-Based Access Control Models, *IEEE Computer*, vol. 29, no. 2, pp. 38-47, Feb. 1996.

[8] M. Sloman, and J. Moffett, Domain model of autonomy, in *Proc. 3rd ACM SIGOPS European Workshop: Autonomy or interdependence in Distributed Systems?*, pp. 1-4, Sept. 1988.

[9] J. Moffett, and M. Sloman, Policy hierarchies for distributed system management, *IEEE JSAC*, vol.11, No. 9, pp. 1404-1414, Dec. 2003.

[10] K. Feeney, D. Lewis, and V. Wade, Policy Based Management for Internet Communities, *Proc. 5th IEEE Int'l Workshop on Policies for Distributed Systems and Networks (Policy 2004)*, pp. 23-34, 2004.

[11] R. Alfieri, et al., VOMS: an authorization system for virtual organizations, *Proc. 1st European Across Grids Conference*, pp. 33-40, 2003.

[12] H. Zhou, and S. N. Foley, A Framework for Establishing Decentralized Secure Coalitions, *Proc. IEEE Computer Security Foundations Workshop*, 2006.

[13] S. N. Foley, and H. Zhou, Authorisation Subterfuge by Delegation in Decentralised Networks, *Proc. 13th Int'l Security Protocols Workshop*, 2005.

[14] J. E. López de Vergara, V. A. Villagr, and J. Berrocal, Applying the Web Ontology Language to management information definitions, *IEEE Commun. Mag.*, vol. 42, no. 7, pp. 68-74, July 2004.

[15] J. Keeney, D. Lewis, D. OSullivan, A. Roelens, A. Boran, and R. Richardson, Runtime Semantic Interoperability for Gathering Ontology-based Network Context, *Proc. IEEE/IFIP Network Operations and Management Symp. (NOMS 2006)*, pp. 55-66, 2006.

[16] N. Noy, Semantic Integration: A Survey of Ontology-Based Approaches, *SIGMOD Record*, vol. 33, iss. 4, pp. 65-70, ec. 2004.

[17] D. OSullivan, V. Wade, and D. Lewis, Understanding as We Roam, *IEEE Internet Computing*, vol. 11, no. 2, pp. 26-33, Mar/Apr 2007.

[18] S. Davy, B. Jennings, and J. Strassner, "The Policy Continuum - Policy Authoring and Conflict Analysis," *Comp. Commun.*, vol. 31, no. 13, pp. 2981-2995, 2008.

[19] S. Balasubramaniam, D. Botvich, B. Jennings, S. Davy, W. Donnelly and J. Strassner, Policy-constrained Bio-inspired Processes for Autonomic Route Management, to appear, *Comp. Netw.*, accepted August 2008.

[20] Autonomic Communication Forum, [Online], Available (26/3/2009): <http://www.autonomic-communication-forum.org/>.

[21] FAME Strategic Research Cluster, [Online], Available (26/3/2009): <http://www.fame.ie>.