INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Madynes

Management of Dynamic Networks and Services

Lorraine

THEME COM

Activity Report

2005

Table of contents

1. Team

MADYNES is a project group of the LORIA (UMR 7503) laboratory, jointlab of CNRS, INRIA, Henri Poincaré University - Nancy 1, Nancy 2 University and the Lorraine National Polytechnic Institute (INPL).

This report covers the group activity from January, 1st 2005 to November 30th, 2005.

Head of the project team

Olivier Festor [Research Director - INRIA]

Vice-head of the project team

Isabelle Chrisment [Associate Professor - HDR, ESIAL, Henri Poincaré - Nancy 1 University]

Administrative Assistant

Josiane Reffort [Project Assistant, Faculté des Sciences, Henri Poincaré - Nancy 1 University]

INRIA Staff

Radu State [Researcher - INRIA]

University Staff

Laurent Andrey [Associate Professor, Nancy 2 University until 31/08/2005, on sabbatical at INRIA since 1/09/2005]
Laurent Ciarletta [Associate Professor, ENSMN - Lorraine National Polytechnic Institute]
Jacques Guyard [Professor, ESIAL, Henri Poincaré - Nancy 1 University]
Emmanuel Nataf [Associate Professor, Nancy 2 University]
André Schaff [Professor, ESIAL, Henri Poincaré - Nancy 1 University]

Project Technical Staff

Frédéric Beck [Engineer, funded by the IST 6Net and the RNRT Safecast contracts]
Vincent Delove [Engineer, delegated by CIRIL, from 1/08/2005 to 31/12/2005]

Ph.D. Students

Rémi Badonnel [Industrial grant with regional co-sponsorship, 2nd year]
Mohamed Salah Bouassida [MEN grant, 2nd year]
Vincent Cridlig [Industrial grant with regional co-sponsorship, 2nd year]
Guillaume Doyen [MEN grant, 3rd year]
Abelkader Lahmadi [Industrial grant, 1st year]
Mohamed Nassar [MEN grant, since 1/10/2005]

Post-doctoral Students

Mi-Jung Choi [Pohang University - Postech, Korea, until 31/09/2005]

Student Interns

Najah Shridi [2 months extended MS degree Internship, UHP-Nancy 1, France]
Humberto Jorge Abdelnur [MS Degree Internship, Argentina]
Julien Braure [BS Degree Internship, UHP - Nancy 1, France]
Jérôme Bourdellon [BS Degree Internship, UHP - Nancy 1, France]
Xavier Grandmougin [MS Degree Internship, DEA Informatique, INPL, France]
Mohamed Nassar [MS Degree Internship, DEA Informatique, UHP - Nancy 1, France]

2. Overall Objectives

2.1. Overall Objectives

Keywords: *automated management, benchmarking, dynamic environments, management frameworks, mobile device management, monitoring, network management, provisioning, security, service configuration, service management, telecommunications.*

The goal of the MADYNES research group is to design, to validate and to deploy novel management and control paradigms as well as software novel architectures that are able to cope with the growing dynamicity and the scalability issues induced by the ubiquitous Internet.

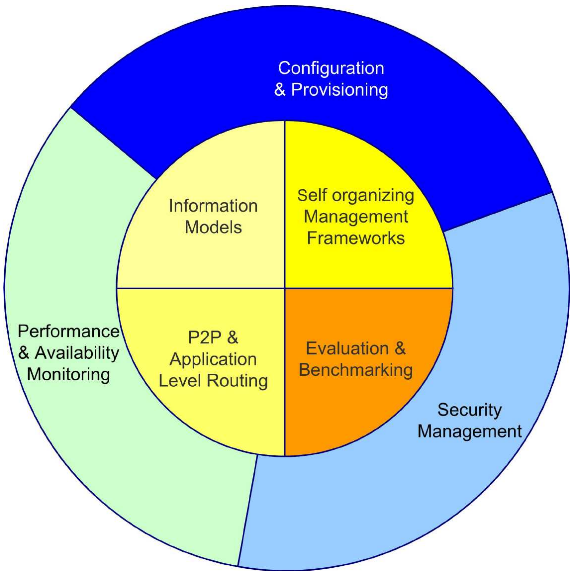

Figure 1. The MADYNES research themes

The project develops research activities in the following areas (see Figure 1):

- **Autonomous Management** (inner circle of Figure 1):
  - the design of models and methods enabling **self organisation and self-management** of networked entities and services,
  - the design and evaluation of management architectures based on **peer-to-peer and overlay principles**,
  - the investigation of novel approaches to the representation of **management information**,
  - the modelling and **performance evaluation** of management infrastructures and activities.
- **Functional Areas** instanciate autonomous management functions (outer circle of Figure 1):
  - the **security plane** where we focus on new key management protocols and security of the management plane,
  - the **service configuration and provisioning plane** where we aim at providing solutions for the automation of processes ranging from service subscription to service deployment and service activation,
  - **performance and availability monitoring**.

The next generation Internet is the main application field of our research. Its architecture and the services that it is planned to support offer all dynamic and scalability features that we address in the two complementary research directions of the project.

3. Scientific Foundations

3.1. Evolutionary needs in network and service management

The foundation of the MADYNES research activity is the ever increasing need for automated monitoring and control within networked environments. This need is mainly due to the increasing dependency of both people and goods towards communication infrastructures as well as the growing demand towards services of higher quality. Because of its strategic importance and crucial requirements for interoperability, the management models were constructed in the context of strong standardisation activities by many different organisations over the last 15 years. This led to the design of most of the paradigms used in today's deployed approaches. These paradigms are the Manager/Agent interaction model, the Information Model paradigm and its container, together with a naming infrastructure called the Management Information Base. In addition to this structure, five functional areas known under the FCAPS[1] acronym are associated to these standards.

While these models were well suited for the specific application domains for which they were designed (telecommunication networks or dedicated protocol stacks), they all show the same limits. Especially they are unable:

1. to deal with any form of dynamicity in the managed environment,
2. to master the complexity, the operating mode and the heterogeneity of the emerging services,
3. to scale to new networks and service environments.

These three limits are observed in all five functional areas of the management domain (fault, configuration, accounting, performance and security) and represent the major challenges when it comes to enable effective automated management and control of devices, networks and services in the next decade.

MADYNES addresses these challenges by focusing on the design of management models that rely on inherently dynamic and evolving environments. The project is centered around two core activities. These activities are, as mentioned in the previous section, the design of an autonomous management framework and its application to three of the standard functional areas namely security, configuration and performance.

3.2. Autonomous management

3.2.1. Models and methods for a self-management plane

Self organisation and automation are fundamental requirements within the management plane in today's dynamic environments. It is necessary to automate the management processes and enable management frameworks to operate in time sensitive evolving networks and service environments. The automation of the organization of devices, software components, networks and services is investigated in many research projects and has already led to several solution proposals. While these proposals are successful at several layers, like IP auto-configuration or service discovery and binding facilities, they did not enhance the management plane at all. For example, while self-configuration of IP devices is commonplace, no solution exists that provides strong support to the management plane to configure itself (e.g. finding the manager to which an agent has to send traps or organizing the access control based on locality or any other context information). So, this area represents a major challenge in extending current management approaches so that they become self-organized.

Our approach is bottom-up and consists in identifying those parameters and framework elements (manager data, information model sharing, agent parameters, protocol settings, ...) that need dynamic configuration and self-organisation (like the address of a trap sink). For these parameters and their instantiation in various management frameworks (SNMP, Netconf, WBEM, ...), we investigate and elaborate novel approaches enabling fully automated setup and operation in the management plane.

Design and evaluation of P2P-based management architectures

[1] Fault, Configuration, Accounting, Performance and Security

Over the last years, several models have emerged and gained wide acceptance in the networking and service world. Among them, the overlay networks together with the P2P paradigms appear to be very promising. Since they rely mainly on fully decentralised models, they offer excellent fault tolerance and have a real potential to achieve high scalability. Mainly deployed in the content delivery and the cooperation and distributed computation disciplines, they seem to offer all features required by a management framework that needs to operate in a dynamic world. This potential however needs an in depth investigation because these models have also many characteristics that are unusual in management (e.g. a fast and uncontrolled evolution of the topology or the existence of a distributed trust relationship framework rather than a standard centralised security framework).

Our approach envisions how a complete redesign of a management framework is done given the characteristics of the underlying P2P and overlay services. Among the topics of interest we study the concept of management information and operations routing within a management overlay as well as the distribution of management functions in a multi-manager/agent P2P environment. The functional areas targeted in our approach by the P2P model are network and service configuration and distributed monitoring. The models are to be evaluated against highly dynamic frameworks such as ad-hoc environments (network or application level) and mobile devices.

3.2.2. Integration of management information

Representation, specification and integration of management information models form a foundation for network and service management and remains an open research domain. The design and specification of new models is mainly driven by the appearance of new protocols, services and usage patterns. These need to be managed and exposed through well designed management information models. Integration activities are driven by the multiplication of various management approaches. To enable automated management, these approaches need to inter-operate which is not the case today.

The MADYNES approach to this problem of modelling and representation of management information aims at:

1. enabling application developers to establish their management interface in the same workspace, with the same notations and concepts as the ones used to develop their application,
2. fostering the use of standard models (at least the structure and semantics of well defined models),
3. designing a naming structure that allows the routing of management information in an overlay management plane, and
4. evaluating new approaches for management information integration especially based on management ontologies and semantic information models.

3.2.3. Modelling and benchmarking of management infrastructures and activities

The impact of a management approach on the efficiency of the managed service is highly dependent on three factors:

- the distribution of the considered service and their associated management tasks,
- the management patterns used (e.g. monitoring frequency, granularity of the management information considered),
- the cost in terms of resources these considered functions have on the managed element (e.g. method call overhead, management memory footprint).

While the first factor was investigated in several research projects so far, none of the other two were investigated at all. The lack of such benchmarking data and models simply make the objective evaluation of the operational costs of a management approach impossible. This may be acceptable in backbone networks where processing and communication resources can be tuned very easily (albeit sometimes at a non negligible cost). This is not true in constrained environments like devices constrained by battery or processing power as found in wireless networks for which the lack of management cost models is a serious concern.

MADYNES addresses this problem from multiple viewpoints: communication patterns, processing and memory resources consumption. Our goal is to provide management patterns combining several management technologies if needed so as to optimise the resources consumed by the management activity imposed by the operating environment.

Therefore, we establish *abacuses* for management frameworks and in parallel we collect data on current management practice. These data will form the core of the "Constraints-based management tuning activity" that we are working on and can be used for rigorous comparison among distribution and processing of management activities.

3.3. Functional Areas

3.3.1. Security: key management protocols and security of the management plane

Securing the management plane is vital. While several proposals are already integrated in the existing management frameworks, they are rarely used. This is due to the fact that these approaches are completely detached from the enterprise security framework. As a consequence, the management framework is "managed" separately with different models; this represents a huge overhead. Moreover the current approaches to security in the management plane are not inter-operable at all, multiplying the operational costs in a heterogeneous management framework.

The primary goal of the research in this activity is the design and the validation of a security framework for the management plane that will be open and capable to integrate the security services provided in today's management architectures. Management security interoperability is of major importance in this activity.

Our activity in this area aims at designing a generic security model in the context of multi-party / multi-technology management interactions. Therefore, we develop research on the following directions:

1. Abstraction of the various access control mechanisms that exist in todays management frameworks. We are particularly interested in extending these models so that they support event-driven management, which is not the case for most of them today.
2. Extention of policy and trust models to ease and to ensure coordination among managers towards one agent or a subset of the management tree. Provisional policies are of great interest to us in this context.
3. Evaluation of the adequacy of key distribution architectures to the needs of the management plane as well as selecting reputation models to be used in the management of highly dynamic environments (e.g. multicast groups, ad-hoc networks).

A strong requirement towards the future generic model is that it needs to be instantiated (with potential restrictions) into standard management platforms like SNMP, WBEM or Netconf and to allow interoperability in environments where these approaches coexist and even cooperate. A typical example of this is the security of an integration agent which is located in two management worlds.

3.3.2. *Configuration: automation of service configuration and provisioning*

Configuration covers many processes which are all important to enable dynamic networks. Within our research activity, we focus on the operation of tuning the parameters of a service in an automated way. This is done together with the activation topics of configuration management and the monitoring information collected from the underlying infrastructure. Some approaches exist today to automate part of the configuration process (download of a configuration file at boot time within a router, on demand code deployment in service platforms, ...). While these approaches are interesting they all suffer from the same limits, namely:

1. they rely on specific service life cycle models,
2. they use proprietary interfaces and protocols.

These two basic limits have high impacts on service dynamics in a heterogeneous environment.

We follow two research directions in the topic of configuration management. The first one aims to establish an abstract life-cycle model for either a service, a device or a network configuration and to associate with this model a generic command and programming interface. This is done in a way similar to what is proposed in the area of call control in initiatives such as Parlay or OSA.

In addition to the investigation of the life-cycle model, we work on technology support for distributing and exchanging configuration management information. Especially, we investigate policy-driven approaches for representing configuration and constraints while we study XML-based protocols for coordinating distribution and synchronisation. Off and online validation of configuration data is also part of this effort.

3.3.3. *Performance and availability monitoring*

Performance management is one of the most important and deployed management function. It is crucial for any service which is bound to an agreement about the expected delivery level. Performance management needs models, metrics, associated instrumentation, data collection and aggregation infrastructures and advanced data analysis algorithms.

Today, a programmable approach for end-to-end service performance measurement in a client server environment exists. This approach, called Application Response Measurement (ARM) defines a model including an abstract definition of a unit of work and related performance records; it offers an API to application developers which allows easy integration of measurement within their distributed application. While this approach is interesting, it is only a first step toward the automation of performance management.

We are investigating two specific aspects. First we are working on the coupling and possible automation of performance measurement models with the upper service level agreement and specification levels. Second we are working on the mapping of these high level requirements to the lower level of instrumentation and actual data collection processes available in the network. More specifically we are interested in providing automated mapping of service level parameters to monitoring and measurement capabilities. We also envision automated deployment and/or activation of performance measurement sensors based on the mapped parameters. This activity also incorporates self-instrumentation (and when possible on the fly instrumentation) of software components for performance monitoring purpose.

4. Application Domains

4.1. Mobile, ad-hoc and constrained networks

The results coming out from MADYNES can be applied to any dynamic infrastructure that contributes to the delivery of value added services. While this is a potentially huge application domain, we focus on the following environments at the network level:

1. multicast services,
2. ad-hoc networks,

3. mobile devices and IPv6 networks.

All these selected application areas exhibit different dynamicity features. In the context of multicast services we focus on distribution, monitoring and accounting of key distribution protocols. On *ad -hoc* and dynamic networks we are investigating the provisioning, monitoring, configuration and performance management issues.

Concerning mobile devices, we are interested in their configuration, provisioning and monitoring. IPv6 work goes on in Information Models and, combined with SNMPv3, on self-configuration of the agents.

Value added services such as virtual private networks (VPN) or voice, video, security services are of interest to the team too.

4.2. Dynamic service infrastructures

At the service level, dynamics is also increasing very fast. We apply the results of our work on autonomous management on infrastructures which support dynamic composition and for which self-instrumentation and management automation is required.

The target service environments are:

- the Open Services Gateway initiative,
- Web Services,
- peer-to-peer infrastructures.

5. Software

5.1. EnSuite: an extended Netconf framework

Participants: Jérôme Bourdellon, Humberto Jorge Abdelnur, Vincent Cridlig, Olivier Festor, Radu State [contact].

EnSuite is the first open source implementation of a full Netconf (Network Configuration protocol) compliant Framework [44]. EnSuite consists of a Netconf web-based manager, a Netconf agent and a set of extension modules. All these components are implemented in Python. YencaPMananager is the management application [39]. It has a simple but powerful web-based GUI. YencaP is a Netconf agent implementation. It supports the addition of new modules as well as new operations that were added in 2005. EnSuite now manages BGP configurations on routers through the XBGP-MAN module. EnSuite is also able to handle remote configuration of VoIP Asterisk environments through a dedicated module [31].

EnSuite is listed on the IETF Netconf list and has been successfully tested in the Interop Event that took place in August 2005 in the context of the IETF meeting in Paris. It was also successfully presented at both the IRTF NMRG (International Research Task Force Network Management Research Working Group) meeting in July 2005 and at the IEEE International Conference on IP Operations an Management Symposium in october 2005 [21].

The entire framework has been registered at the APP agency [50] and is available on the group's web page for download.

5.2. JDukeBox

Participants: Frédéric Beck [contact], Mohamed Salah Bouassida, Vincent Delove, Isabelle Chrisment, Olivier Festor, Abdelkader Lahmadi.

JDukebox is a distributed cooperative jukebox. It enables users to share music and listen to an incrementally built distributed playlist. JDukebox operates in a fully distributed way on top of a peer-to-peer infrastructure (here JXTA). Communication among the peers is ensured for the signaling part through JXTA channels and for the content delivery through native IPv6 multicast. All communications among entities are secured including the group communications. The Balade protocol for key distribution is used for this purpose. The SOCT-2 protocol was implemented in the tool to provide the playlist consistency service.

The environment is freely distributed and serves as a demonstrator for various management components issued from the team (P2P management framework, key distribution protocols for dynamic environments). JDukebox was demonstrated at the JRES days in Marseille in December 2005 on top of Mobile IPv6 in a mobile environment. The software is distributed over the libresource forge.

6. New Results

6.1. Securing the management plane

Participants: Vincent Cridlig, Olivier Festor, Radu State [contact].

The emergence of multiple management protocols and management interfaces over the recent years raises new and important challenges to the security of the management plane. The main challenges are related to (1) the scalability required to cope with the multiplicity of managed devices and dynamic manager to agent interaction and (2) providing a good and uniform security level independently of the management interface/protocol.

Assuring the security of the management plane is one of the main research activities of our group. Our research activity focuses on providing a uniform security continuum independent on the underlying management protocol and interface.

In 2005, we worked on two main issues, namely global and local consistency of security policies. Global consistency, which means consistency between equivalent groups of devices like BGP routers, can be achieved by a two steps process: first define a central policy and then deploy it automatically in a large scale network. Local consistency, which consists of having the same rights whatever the framework and access protocol used to manage one device is, can be achieved in two different ways. First, a convergence API can be defined between the management framework and the managed operating system. The management framework then delegates the access control to this API which is common to all management interfaces offered by a given device (SNMP, CLI, Netconf, ...). Second, algorithms can be designed to map a framework-independant policy to the different frameworks of a single device (e.g. map SNMP USM/VACM to Netconf RBAC policies or CLI security levels).

We have designed a set of architectural elements adressing these issues:

- A **security architecture for the global consistency of Netconf based on Role-Based Access Control (RBAC)** [22]. Encryption and Authentication key management is done through multicast communication, with a bijection between multicast groups and RBAC activated roles. RBAC sessions management is centralized in a key distribution center;
- A **mapping algorithm from RBAC roles to CLI security levels**. Weights are assigned to RBAC roles in order to gather roles into subsets (using the K_Means_Clustering algorithm) and to map these subsets to the CLI security levels;
- **A RADIUS/SNMP collaborative architecture**. RADIUS is used to deploy the access control rules to the SNMP agents [23], [24]. The agents use the manager credentials to retrieve the allowed roles from he RADIUS server. It enables a centralized processing of part of the access control policy and therefore minimizes the maintenance costs.

An experimental performance evaluation has been done to observe the behaviour of Netconf under various security approaches (XML-Encryption vs SSH, AES vs 3DES, impact of access control) and with different Netconf methods or extensions (compression, data model filtering, modules).

We have also undertaken some work to ensure the integrity of Netconf device configuration. It enables the detection of anomalies coming from unauthorized updates to the XML configuration. Our approach is based on digital signatures of the configuration to enable the configuration integrity check at any time by computing a footprint and compare it with the signed hash value. We are extending this model in the context of multi-provider environments.

6.2. Secure multicast in ad-hoc networks

Participants: Mohamed Salah Bouassida, Isabelle Chrisment [contact], Olivier Festor.

We are working on the design of authentication and key distribution protocols that satisfy the strong constraints imposed by the combination of ad-hoc networks and multicast communications. Securing multicast communications in ad-hoc networks must meet several challenging factors such as high mobility of nodes, limited bandwidth and constrained energy. Moreover, the establishment of a key management protocol within ad-hoc environments meets the "1 affects n" problem, which is critical in such types of networks, due to the high dynamicity of groups.

We have designed a **clustering scheme for multicast key distribution in mobile ad-hoc networks**. This scheme called OMCT (*Optimize Multicast Cluster Tree*). This scheme divides the multicast group into clusters, according to the localization of the group members and their mobility. Simulations indicate a valuable reduction in the average latency of keys distribution and a promising reduction in energy consumption [16].

Then, we have defined a **new key management protocol for secure multicast communications, dedicated to operate in ad-hoc networks**. This framework, called BALADE, delivers a fast, efficient and mobility aware key distribution scheme in a multicast service in which sources follow themselves in a sequential way [15].

We have designed the **integration of the OMCT algorithm within our group key management protocol BALADE**. Our integration model allows an efficient and fast key distribution process which takes into account the nodes localization and mobility; it also optimizes the energy and bandwith consumptions. This efficiency was validated through simulations on different mobility models [17].

6.3. Management benchmarking

Participants: Laurent Andrey [contact], Olivier Festor, Abdelkader Lahmadi.

In 2005, the activity around management benchmarking has been extended to *performance analysis of networks and services management framework*. This activity led to three major achievements in addition to the production of a large state of the art on the performance analysis of networks and services management frameworks [46].

The first achievement is the **design and execution of a rigorous measurement campaign on Java-based management components**. Using the test suite initiated last year, we conducted a first series of *synthetic* performance tests (benchmarks) to evaluate how a single JMX agent scales when request injection rate increases. We also investigated some other scaling factors such as: number of MBeans (components) instanciated into the agent, number of attributes exposed by the MBeans. These results have been published in [29]. A first version of the test suite description has been released in [33]. The corresponding code is freely available on the teams' web page.

The second achievement in benchmarking is the **definition of a metric that captures the impact of the management plane on the functional plane**. We there adressed the following issue: *How does the management plane interfere with the functional plane?* We adapted concepts from distributed systems community [53], [51] and we defined an *impact metric* where the production of the functional plane is linked with the production of the management plane considering the overall resources consumption.

We conducted a first validation of the proposed metric by setting a benchmark. For the functional plane we use the realistic benchmark *Rubis* [52] where we inject synthetic management activities by reusing elements we have developed for the first point. Thus we calculate the value of our impact metric for several test factors. It appears that the running areas where management impact is acceptable (according to our metric) still allows enough management operations (expressed in number of management attributes read per second) for usual monitoring activities. This work has been published in [28].

The third result is the **extension of our performance test suite**.

The initial test suite has been extended by:

- manager side tests. Scenarii where one manager interacts with many agents have been designed and implemented. For this activity we use largely INRIA's i-cluster located at the Grenoble premises;

- support of a notication service. For now, only the usual *get service* has been tested. Some scenarii for the asynchronous notification delivery services and higher level monitoring services (*gauges*, *counters*) have also been designed;
- support of SOAP[2]. We introduced a new test factor in the test suite namely the type of the underlying connectivity between managers and agents. Code for SOAP connector has been written in addition to the existing one for RMI/JRMP[3]

6.4. Management of peer-to-peer overlays

Participants: Guillaume Doyen, Olivier Festor [contact], Julien Braure, Emmanuel Nataf.

New results in the MADYNES peer-to-peer (P2P) management research activities are related to previous work within the team on Distributed Hash Table (DHT) management and to others coming from studies performed during the year 2005.

The first achievement concerns the **performance management of P2P DHT** [26]. This contribution extends the generic P2P management information model we proposed last year. Such performance management is needed because of the large scale of DHT-based P2P networks and their high dynamicity (ie. peers moving in and out of the network). The contribution includes:

- new information models defined for the performance management of:
  - request lookups that are sent for the retrieval of resources in the DHT and that are forwarded from peer to peer until they reach the peer node containing the resource location,
  - the maintenance process of the global routing plan that is distributed among all peers and that needs to be reorganized each time a peer comes up or leaves the network.

  Theses elements have been provided for compatibility reasons as extensions of the standard “unit of works” defined in the Common Information Model (CIM).
- a new generic information model defined to describe a DHT peer and a DHT community. It comes from our previous P2P peer and P2P community models;
- the instrumentation of the performance information model realized by the definition of some points of measurement in the request lookup process that occurs in each peer on the way of such request. Collected data are gathered by a standard-based DHT unit of work correlator and are summarized to give performance information in term of:
  - average number of hops for a lookup request,
  - global response time from the request to the response (success or failure),
  - request cost in term of number of messages exchanged,
  - computation time, including local cache search and routing process.

A hierarchical architecture for P2P network management is a new contribution to the network management domain. We base our proposal on pure P2P systems, that are neither hybrid, half-hybrid or centralized P2P networks. In such a very dynamic environment, it is very difficult, even impossible, to deploy a management function on several peers with a usual client/server management architecture. As a peer can leave/join the network at any time, it makes no sense to assign to it a management role definitively, neither the manager (client) nor the agent (server) one. We have defined a classification of P2P environments based on their manageability. This work [27] was done on the base of several features:

[2] Simple Object Access Protocol http://www.w3.org/TR/soap/

[3] Remote Method Invocation/Java Remote Method Protocol

- openness to the management by a dedicated interface,
- decentralization of the P2P network,
- support by an overlay network,
- scale and dynamicity of the P2P network.

We propose a self-organizing hierarchical architecture to manage large number of network nodes. The originality of our approach is to dynamically assign a role to a part of the present peers and so to be able to react to any change of peer participation. Roles of peers are either top or intermediate manager. In addition, each peer must provide agent capabilities. Depending on their identifier, peers are placed in the management tree in order to manage peers with a common identifier prefix. The hierarchy could be reorganized when peers come in and out of the P2P network or when a new powerful peer (CPU or bandwith criteriums could be used) may replace an existing manager.

The implementation of our management architecture is made on the DHT based P2P network *freePastry*. As such a dynamic architecture leads to several message exchanges for organizing the management tree, and in order to test our implementation, we first focused on providing load measurement based on the number of messages exchanged when the number of peers increases [25]. We plan to test the scalability of our architecture on a more powerful simulation tool with thousand peers.

6.5. Monitoring and management of ad-hoc networks

Participants: Rémi Badonnel, Olivier Festor, André Schaff, Radu State [contact].

The main research activities on the management of dynamic ad-hoc networks were focused on the identification of the management information required in the context of ad-hoc networks and on underlying management architectures. With respect to the first activity, we have defined an **information model capable to represent management data for the spatial, temporal and traffic aspects**. Thus, the accurate and comprehensive representation of parameters which drive the evolution of an ad-hoc network, is possible. Among the represented information, we defined in [14], [8] an end-to-end metric providing a global measure of the transport level connectivity available in an ad-hoc network. We analyzed the impact of several factors like mobility, routing protocol and density of the networks, in order to determine the role and degree of importance of each of them. We proposed in the above mentioned work the **extension of a SNMP based management architecture** (ANMP) as a potential supporting management framework. Our extension consists in the definition of a inter-cooperation protocol based on SNMP for mid-level managers and in a MIB extension for the metrics. Based on a comprehensive set of simulations, we were able to define a management protocol that configures the routing protocol in order to achieve optimum global end-to-end transport level connectivity [9]. We have presented the complete information model in [8] and specified a first draft of a MIB module for the OLSR routing protocol.

The second research activity addressed the **supporting management architectures for an ad-hoc network**. The major issue is how to use the management information in order to do fault management or to detect malicious nodes. This task is very difficult in an ad-hoc network context. While fault detection in fixed wired networks is not hindered by the impossibility to observe a given node, ad-hoc networks specifics do provide major challenges with respect to this issue. A node that does not reply to legitimate polling in a fixed network is typically considered as not functional. In an ad-hoc network, observability is a major issue: a node might not be reachable because he is moving and/or out of reachability, or because it is not functioning properly. A centralized manager/agent architecture is not viable for ad-hoc network, because the manager itself might become isolated or resource exhausted. Resource consumption due to management is neglected in fixed networks, while the issue is of major importance in a context where bandwidth and battery lifetime are the key actors. Trust is another main issue, since nodes might not provide reliable data or might voluntarily corrupt it and report wrong data. Our work addressed the issue of passive and lightweight monitoring of ad-hoc networks. We designed **an original method based on the eigenvector decomposition and information theoric**

measures of monitored management data in order to detect nodes that are particular [12], [36], [34]. This particularity can be positive (for instance nodes that do important routing and constitute the equivalent of traffic highways in ad-hoc networks) or negative (for instance nodes that flood the network, without providing a minimum of service to it). We proposed and evaluated a detection mechanism based on image processing filtering techniques such that both abnormal nodes and traffic highways are well identified.

6.6. Autonomous management

Participants: Laurent Ciarletta [contact], Olivier Festor, Mi-Jung Choi.

In 2005, we focused our work on self-organization of the management around the Swan project. We did focus on the use of XML-based approaches to configuration management. A state of the art in network configuration has been established [43]. Using the definition of a self-organizing management plane that we developed last year, we proposed a management framework and algorithm and we did apply it to **automated Virtual Private Networks (VPN) provisioning**. A prototype implementation of the autoconfiguration of VPNs has been developed [18];

We also proposed a solution for the **autoconfiguration of the entities pertaining to the management plane using service discovery protocols** [20] that could be integrated within the general framework of Swan.

6.7. Pervasive computing

Participants: Laurent Ciarletta [contact], Olivier Festor.

Pervasive computing, where a growing number of computing devices are collaborating to provide users with enhanced and ubiquitous services, is a domain that we are currently exploring. It has a lot of different requirements. The following ones are specifically related to the work done within Madynes:

- an adaptable yet high level of security is needed since these computing devices should be working in such a way common users trust themselves,
- pervasive Computing is high technology seamlessly woven into our everyday life: therefore it requires autoconfiguration and reconfiguration of its elements and networks,
- the technologies need to be evaluated not only per domain, but on a larger scale, where end-user concerns are also taken into account.

We are investigating this domain and did provide a first contribution, namely a simple secure infrastructure for access control to Pervasive Computing environments together with a framework for evaluating the technologies involved by using a combination of emulation and real elements [19].

7. Contracts and Grants with Industry

7.1. AMARILLO

Participants: Laurent Andrey, Abdelkader Lahmadi, Olivier Festor, Emmanuel Nataf [contact].

Dates	December 2003 - June 2005
Partners	Thalès (leader), INRIA-MADYNES, LIP6, ENST, Paris XIII University.

AMARILLO is a research project funded by the French National Research in Telecommunications (RNRT) agency. The goal of the project is to investigate novel application domains for highly distributed active environments and to evaluate these environements on several test platforms.

The MADYNES contributions to this project are:

- a study on management benchmarking and the evaluation of distributed management algorithms,
- the design of a component-based management agent using the Model Driven Architecture (MDA) approach.

This work is part of the benchmarking and self-organizing management plane themes of the MADYNES team. This project was completed on June 2005.

7.2. SAFARI

Participants: Rémi Badonnel, Julien Braure, Mohamed Salah Bouassida, Isabelle Chrisment, Guillaume Doyen, Olivier Festor [contact], Radu State.

Dates February 2003 - January - April 2006

Partners France Télécom (leader), ALCATEL, INRIA (ARES, HIPERCOM, MADYNES), LIP6, LRI, LSIIT, LSR-IMAG, SNCF and ENST.

SAFARI is precompetitive research project funded by the French National Research in Telecommunications (RNRT) agency. The goal of the project is to design, to setup and to deploy a communication suite enabling transparent access, automated configuration, service integration and adaptation within an IPv6 ad-hoc network that maintains connectivity with the Internet.

The MADYNES contributions to this project are:

- the design of a policy-based approach for bandwidth reservation in the ad-hoc part of the network,
- the design of a monitoring architecture enabling dynamic reconfiguration and supporting transient connectivity of monitored and monitoring nodes,
- the design of a key distribution architecture dedicated to secure a multicast service within the hybrid network.

This work is part of the performance management, security management and information modeling themes of the MADYNES group. In 2005 we continued the integration of our management algorithms with the routing schemes used in SAFARI (OLSR). This led to the design of an OLSR MIB module. We also continued our investigations on key distribution models for multicast communications in ad-hoc environments. We also worked on the instrumentation of the JXTA platform to provide service level management facilities at the middleware level [40]. We are now working on the final prototype which will be delivered and demonstrated at the end of the project.

7.3. SAFECAST

Participants: Isabelle Chrisment [contact], Mohamed-Salah Bouassida, Olivier Festor.

Dates March 2004 - February 2007

Partners EADS (leader), LAAS-CNRS, ENST, INRIA (MADYNES) and Heudiasyc UTC Compiègne

SAFECAST is a research project funded by the French National Research in Telecommunications (RNRT) agency. The goal of the project is to develop a global secure architecture for group communication within an environment where every member can be a sender and a receiver. The security of group communication is to be provided while allowing dynamicity of receivers. Each receiver can join or leave a group at any time.

The main MADYNES contributions to this project are:

- the design of a group key management protocol,
- the validation and simulation of the proposed protocol.

This work is part of the security management and self-organization of the management plane themes of the MADYNES group. In 2005, we contributed to the writing of the state of the art related to the different algorithms used in multicast cryptography [32] and also to the state of the art of the group key management in wired and ad-hoc networks [37].

In collaboration with the University of Compiègne, we defined a hierarchical key distribution protocol adapted to the PMR (*Professional Mobile Radio*) application proposed by EADS in the context of SAFECAST [38].

We have formaly specified the proposed group key distribution solution by integrating the management of certificates for authentication and access control. The whole approach is composed of different operations (join, leave, merge, split,...) which have been described in the HLPSL (*High Level Protocol Specification Language*) language in order to be validated, in terms of security, through the AVISPA tools [42].

7.4. IST-6Net

Participants: Frédéric Beck, Isabelle Chrisment [contact], Olivier Festor.

Dates January 2002 - June 2005

Partners CISCO (leader), IBM, European NRENs, 12 universities and labs.

6NET (Large-scale International Ipv6 Pilot Network) is an IST project of the 5th framework with 30 participants. The project aims at deploying and operating a native IPv6 backbone throughout Europe to experiment all IPv6 services in an inter-domain environment on a large scale.

The MADYNES contribution to this project is the evaluation of management algorithms in the context of IPv6 and the evolution of Open Source management platforms to support IPv6.

Within 6Net, we designed a new algorithm for the discovery of IPv6 Local Area Networks topologies. We implemented the IPv6 MIB-2 on the net-snmp framework and ported several environments on IPv6 (NAGIOS, NTOP, Looking glass services).

In 2005, we concentrated our efforts on the study of the renumbering operation and its impact on the management of dynamic IPv6 networks. This study has led to the design of a distributed monitoring framework named NetSV which enables a central manager to follow in near-real time the evolution of a renumbering procedure and in case of failure to remotely diagnose the reasons why systems did not perform an announced renumbering. The system was successfully demonstrated at the end of the project and a follow-up to this investigation has started in our group in cooperation with Cisco Systems.

This work is part of the self-organization of the management plane theme of the MADYNES team.

6Net was successfully completed in June 2005.

7.5. MUSE

Participant: Olivier Festor [contact].

Dates January 2004 - December 2005

Partners Alcatel (leader), 10 universities, 5 system vendors, 2 component vendors, 8 telecom operators, 2 SMEs.

MUSE is an IST project funded by the european commission within the 6th framework. The overall objective of MUSE is the research and development of a future low-cost, full-service access and edge network, which enables the ubiquitous delivery of broadband services to every European citizen. The project addresses the network architecture, techno-economics, access nodes, solutions for the first mile, and interworking with the home network. Solutions will be evaluated in end-to-end lab trials and promoted in standardisation.

The MADYNES group is contributing to the project under the leadership of Stéphane Frénot from the ARES group to:

- the definition of a multi-service provider management plane for OSGi,
- its evaluation in a large scale environment.

This work is part of the Dynamic Service Infrastructures application domain addressed by the MADYNES team. MADYNES involvment in MUSE will be extended in phase II of the project.

7.6. SWAN: Self aWare mAnagemeNt

Participants: Laurent Ciarletta [contact], Adil El Kaysouni.

Dates January 2004 - June 2006

Partners INRIA (MADYNES), (LIPN) LABRI, QoSMetrics, Alcatel, CIT, IRISA INRIA Rennes, France Telecom R&D

SWAN (Self aWare mAnagemeNt) is a RNRT exploratory project. It proposes to develop and test "self-aware" management methodologies. The project focuses on management by Web Services and Web Services administration, anticipating the actual trend towards the generalization of Web based solutions. In order to achieve its goals, the project identified 3 key working areas:

1. to identify self-aware management issues common in network management and Web Services administration,
2. to investigate mathematical tools (formal framework and algorithms),
3. to test the proposed methodologies within 2 platforms, one for self configuration of network devices and the other for Web Service deployement.

We contribute to:

- the definition of a self-organizing management plane,
- its application to Virtual Private Networks (VPN) provisioning.

The work done within this project is part of both the Information models, configuration management and self-organization of the management plane activities of the MADYNES team.

8. Other Grants and Activities

8.1. International relationships and cooperations

We maintain several international relationships, either through a formal cooperation or on an informal basis.

Olivier Festor is the initiator and the scientific leader of the MAGIX Network of Excellence proposal submitted in the 4th call of the 6th Framework in Europe. MAGIX brings together the best european research teams on management. It is initially built around 13 research teams and one financial coordination entity. The network aims at shaping the European research in the area of device, network and service management to provide the necessary coordination and integration so as to enable the participants, while maintaining and enhancing their excellence in their respective field, to contribute in a unified way to the design of management solutions covering all of the challenges arising in this field.

The MAGIX proposal did successfully pass the selection process and has been selected as a network of excellence. The negociation phase with the commission has ended in october 2005. The network is expected to start in early 2006.

We maintain an informal cooperation with the group of Aiko Pras at the University of Twente, The Netherlands. This cooperation is instanciated mainly through our joint participation to the Internet Research Task Force (IRTF) Network Management Research Group (NMRG) and through joint organisation of network management events. In 2005, we participated to one NMRG meeting (Nancy, July 30 and 31, 2005). This 2 days event was hosted by our group. Its theme was: Voice over IP Management. 17 participants from all over the world did join. Several demos were made including EnSuite and our VoIP security environments.

We are also members of the EUNICE consortium. EUNICE has been established to foster the mobility of students, faculty members and research scientists working in the field of information and communication technologies and to promote educational and research cooperations between its member institutions. The major event of EUNICE is an annual summer school which brings together lecturers, researchers, students and people from the industry across Europe for one week of presentations, discussions and networking. This year Guillaume Doyen gave a presentation during the Summer School on his work on P2P management [26].

MADYNES is also an active member of the STIC-Asia initiative which promotes cooperation between France and several Asian countries, specially in topics linked to the development, deployment and acceptance of IPv6 technology. This project is managed in France by Thomas Noël from the University Louis Pasteur in Strasbourg. The Post-doc of Mi-Jung Choi from Postech, Korea was supported by this initiative.

8.2. National initiatives

In addition to the cooperation with the various partners within national RNRT projects, we also participate to the CNRS pluridisciplinary network (RTP) on communication networks. Olivier Festor is member of the board of this network.

Olivier Festor is member of the board of the Next Generation Internet (ING) CNRS summer school which was held in June 2005 in Montreuil sur mer. The team is regularly contributing to the organization of the school and is a contributor to several tutorials given during the school week. Abdelkader Lahmadi, Vincent Cridlig, Rémi Badonnel and Mohamed Salah Bouassida did participate to this year event.

Olivier Festor is member of the board of the INRIA-Alcatel cooperation as part of the Alcatel research partnership.

Olivier Festor is a member of the “Actions d’Envergure” committee from the COST board at INRIA.

8.3. Guest Researchers

Since october 2004, Mi-Jung Choi has joined the MADYNES group for a one year postdoc. Mi-Jung holds a Ph.D. from Pohang University in Korea and is working on Web-based management frameworks for distributed management solutions. Within MADYNES, she was working on applying XML-based management to advanced internet services of the YENCA Netconf environment towards IPv6 firewalling configuration support. She will continue the investigation of the use of XML-based techniques for autonomous management and their application to VPN management.

9. Dissemination

9.1. Program committees and conference organisation

Alexander Clemm did co-chair with Aiko Pras and Olivier Festor the IFIP/IEEE International Symposium on Integrated Network Management which was held in Nice in May 2005. IM is the flagship conference on network management. 53 papers out of 230 submitted ones were presented at the conference to more than 320 attendees. The proceedings were published by IEEE Press [6].

Isabelle Chrisment was member of the program committee of the following events: SAR 2005 , CFIP 2005, NOTERE 2005, SAPIR 2005 and MCETECH 2005. She is also member of the scientific board of SAR.

In 2005, Olivier Festor was member of the following program committees: IFIP/IEEE IM’2005, IFIP/IEEE NOMS 2005, CFIP’2005, NOTERE 2005, SAPIR 2005, GRES 2005.

Olivier Festor is also member of the Board of Editors of the Journal of Systems and Network Management and reviewed 23 papers for several international conferences and journals in 2005.

Radu State did participate in the technical program committee of the following conferences: SAR'2005, IFIP/IEEE IM'2005, IFIP/IEEE DSOM'2005. He chaired session at IFIP/IEEE IPOM'2005.

9.2. Teaching

There is a high demand on networking courses in the various universities to which the LORIA belongs. This puts high pressure on the MADYNES members which are all in charge of numerous courses in this domain. Especially the team professors and associate professors ensure more than the required amount of teaching obligation in their respective institutions: IUT, DEUG, bachelor, master, ESIAL and École des Mines de Nancy engineering schools or DEA. In this section, we only enumerate the courses that are directly related to our research activity.

Within the Master degree, SDR (Distributed Services and Networks) specialization, Isabelle Chrisment and Olivier Festor are in charge of the course entitled *Routing and Organization within Dynamic Networks*. This course is one of the three foundation courses given to the students that follow a research cursus in Networking in Nancy; Isabelle Chrisment and Radu State are in charge of the course entitled *Security within Dynamic Networks* at the Masters in Computer Science level. Radu State is also giving three advanced courses on Network Security, one entitled *Systems and Network Security* given at the ESIAL Engineering School and at the Masters in Computer Science level, a second course entitled *Viral and Worm Epidemiology* given at the Masters in Computer Science level, and a course entitled *Introduction to Network Security* given at the Bachelor in Computer Science level.

Isabelle Chrisment is heading the Telecommunications and Networks specialization of the 3rd year at the ESIAL[4] engineering school. She also teaches the networking related courses in this cursus.

Olivier Festor and Emmanuel Nataf are in charge of the *Network and Service Management* course and Radu State teaches network security and wireless communications at the masters degree level.

Olivier Festor was co-leader of the Distributed Services and Communication Networks Research specialization of the new Masters of Computer Science proposal for the Universities in Lorraine until September 2005.

André Schaff is the Director of the ESIAL Engineering School.

Laurent Andrey did head of multimedia departement at the IUT in Verdun up to September 2005, when he joined INRIA on sabattical.

Several MADYNES Ph.D. Students gave various course in the area of networking, Java, Web-services and XML technologies, Service Oriented Architectures, Design patterns in most universities and engineering schools associated with the LORIA.

9.3. Tutorials, invited talks, panels, presentations

In addition to the presentation of all papers published in conferences in 2005, the team members made the following presentations:

- Isabelle Chrisment did present the contributions of the team on key distribution protocols for multicast communications in ad-hoc networks during the evaluation day of SAFECAST in July 7th.
- Humberto Abdelnur did present our VOiP security assessment tool at the 13rd IRTF NMRG meeting in July, 30th,
- Vincent Cridlig did present the EnSuite framework during the 13rd IRTF NMRG meeting in July 31th,
- Frédéric Beck did present the NetSV monitoring tool at the 6Net meeting in January.

Olivier Festor was the guest editor for the LORIA Letter number 14 dedicated to the Internet of the future. This letter was published in March 2005. Rémi Badonnel, Mohamed Salah Bouassida, Isabelle Chrisment and Radu State did contribute to this issue.

[4] *Ecole d'Ingénieurs en Informatique et ses Applications de Lorraine*

9.4. Commissions

Following Habilitation Degree defenses were held by members of the team:

- Isabelle Chrisment, Habilitation Degree in Computer Science from the Henri Poincaré University Nancy 1, France, *Maîtrise de la dynamique dans l'Internet - de l'adaptation des protocoles à la sécurité des services* - [7]. Committee: Paul Amer (reviewer), Abdelmadjid Bouabdallah (reviewer), Jean-Jacques Pansiot (reviewer), Olivier Festor, André Schaff et Stéphane Ubéda (chair), october 2005.

Team members did participate to the following Ph.D. commissions:

- Andrey Sadovykh, Ph.D. in Computer Science from the University Pierre et Marie Curie - Paris VI, *Concept innovateur d'un middleware pour la supervision dee systèmes complexes*, Michel Diaz (reviewer), Olivier Festor (reviewer), Serge Fdida, Marie-Pierre Gervais, Antoine Laydier, Ramon Puigjaner, Stefan Wesner, april 2005.
- Nicolas Larrieu, Ph.D. in Computer Science from INSA de Toulouse, *Contrôle de congestion et gestion du trafic à partir de mesures pour l'optimisation de la QdS dans l'Internet*, committee: Serge Fdida (reviewer), Guy Leduc (reviewer), Olivier Festor (chair), Christophe Chassot, Fabrice Guillemin, Philippe Owesarski (advisor), July 2005.
- Mikael Hoerdt, Ph.D. in Computer Science from the University of Strasbourg, *Quelques propositions extensibles et déployables à l'inter-domaine pour le modèle de diffusion multipoint IP à source unique*. Committee: Walid Dabbous (reviewer), Michel Diaz (reviewer), Jurek Korczack (reviewer), Olivier Festor (chair), Dominique Grad, Jean-Jacques Pansiot (advisor), September 2005

MADYNES members were members of the following Habilitation Degree commission:

- Jean-Philippe Martin-Flatin, Habilitation Degree in Computer Science from Pierre et Marie Curie University Paris VI, *Gestion intégrée de réseaux, systèmes et de services*, Olivier Festor (reviewer), Emil Lupu (reviewer), Michel Riveill (reviewer), Frédéric Desprez, Serge Fdida, David Hutchinson, November 2005.

Olivier Festor is member of the SPECIF Ph.D. award jury which awards every year the best Ph.D. in computer science in France. He also serves as an expert for European programs as well as for the french national innovation agency ANVAR.

Since october 2004, Olivier Festor is a nominated member of the hiring committee in Computer Science at the Louis Pasteur University in Strasbourg. He is also a nominated member of the Henri Poincaré - Nancy 1 University since October 2004 of the hiring committee in automation and a nominated suppleant member in the same university in computer science.

Emmanuel Nataf is an elected member of the hiring committee in Computer Science at the University of Nancy 2 (27th section).

André Schaff is a member of the Henri Poincaré - Nancy 1 University hiring committee in Computer Science.

10. Bibliography

Major publications by the team in recent years

[1] R. BADONNEL, R. STATE, O. FESTOR. *Using Information Theoric Measures for Detecting Faulty Behavior in Ad-Hoc Networks*, Technical report, Jun 2005.

[2] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *An Enhanced Hybrid Key Management Protocol for Secure Multicast in Ad Hoc Networks*, in "Third International IFIP-TC6 Networking conference - NETWORKING 2004, Athenes, Greece", N. MITROU, K. KONTOVASILIS, G. ROUSKAS (editors). , Lecture Notes in Computer Science, vol. 3042, Springer-Verlag, May 2004, p. 725-742.

[3] V. CRIDLIG, R. STATE, O. FESTOR. *Role-Based Access Control for XML Enabled Management Gateways*, in "15th IFIP/IEEE Distributed Systems : Operations and Management - DSOM 2004, Davis, CA, USA", A. SAHAI, F. WU (editors). , Lecture notes in Computer Science, vol. 3278, Springer, UC Davis, Nov 2004, p. 183-195.

[4] G. DOYEN, E. NATAF, O. FESTOR. *A hierarchical architecture for a distributed management of P2P networks and services*, in "16th IFIP/IEEE Distributed Systems : Operation and Management - DSOM'05, Barcelona, Spain", Oct 2005.

[5] O. FESTOR. *Ingénierie de la gestion de réseaux et de services : du modèle OSI à la technologie active*, Habilitation à Diriger des recherches, UHP-Nancy 1, Dec 2001.

Books and Monographs

[6] A. CLEMM, O. FESTOR, A. PRAS. *Integrated Management IX : Managing New Network Worlds*, IEEE Press, May 2005.

Doctoral dissertations and Habilitation theses

[7] I. CHRISMENT. *Maîtrise de la dynamique dans l'Internet - de l'adaptation des protocoles à la sécurité des services*, Habilitation à Diriger des recherches, Université Henri Poincaré - Nancy I, Oct 2005, http://tel.ccsd.cnrs.fr/tel-00010870.

Articles in refereed journals and book chapters

[8] R. BADONNEL, R. STATE, O. FESTOR. *Management of Mobile Ad-hoc Networks : Information Model and Probe-based Architecture*, in "ACM International Journal of Network Management", vol. 15, n^o 5, 2005.

[9] R. BADONNEL, R. STATE, O. FESTOR, A. SCHAFF. *A Framework for Optimizing End-to-End Connectivity Degree in Mobile Ad-Hoc Networks*, in "Journal of Network and Systems Management", vol. 13, n^o 4, Dec 2005.

[10] M. BENAISSA, V. LECUIRE, F. LEPAGE, A. SCHAFF. *Efficient DE-Jitter Control for Voice Applications over Wireless Ad Hoc Networks*, in "Telecommunication Systems", vol. 28, n^o 2, Feb 2005, p. 211-230.

[11] O. FESTOR, I. ASTIC. *6Net : An IPv6 Deployment Guide : Contribution to Chapter 7 Network Management*, in "6Net : An IPv6 Deployment Guide", M. DUNMORE (editor). , The 6Net consortium, Sep 2005.

Publications in Conferences and Workshops

[12] R. BADONNEL, R. STATE, O. FESTOR. *Management of Mobile Ad-Hoc Networks : Evaluating the Network Behavior*, in "9th IFIP/IEEE International Symposium on Integrated Network Management - IEEE IM'2005, Nice, France", A. CLEMM, O. FESTOR, A. PRAS (editors). , IEEE Communications Society, Seraphin Calo and Roberto Kung, May 2005, p. 17-30.

[13] R. BADONNEL, R. STATE, O. FESTOR. *Monitoring End-to-End Connectivity in Mobile Ad-Hoc Networks*, in "4th IEEE International Conference on Networking - ICN'2005, Reunion Island, France", P. LORENZ, P. DINI (editors). , Lecture Notes in Computer Science, vol. 3421, Springer, Apr 2005, p. 83-90.

[14] R. BADONNEL, R. STATE, O. FESTOR, A. SCHAFF. *Gestion des réseaux mobiles ad-hoc : évaluer l'impact des noeuds au sein du réseau*, in "11ème Colloque Francophone sur L'Ingénierie des Protocoles - CFIP'2005, Bordeaux, France", R. CASTANET (editor). , Hermes Science, Lavoisier, Apr 2005, p. 333-348.

[15] M. S. BOUASSIDA, A. BRUNETON, A. LAHMADI, I. CHRISMENT, O. FESTOR. *Balade : diffusion multicast sécurisée d'un flux multimédia multi-sources séquentielles dans un environnement ad hoc*, in "Colloque Francophone sur l'Ingénierie des Protocoles - CFIP 2005, Bordeaux, France", R. CASTANET (editor). , Hermes science, Mar 2005, p. 531–546.

[16] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *Efficient Clustering for Multicast Key Distribution in MANETs*, in "NETWORKING 2005 : 4th International IFIP-TC6 Networking Conference, Waterloo, Canada", R. BOUTABA, K. ALMEROTH, R. PUIGJANER, S. SHEN, J. P. BLACK (editors). , Lecture Notes in Computer Science, vol. 3462, Springer-Verlag, May 2005, p. 138-153.

[17] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *Prise en compte de la mobilité dans le protocole de gestion de clé de groupe BALADE*, in "4th Conference on Security and Network Architectures - SAR 2005, Batz sur Mer, France", M. ACHEMLAL, M. MAKNAVICIUS (editors). , Jun 2005, p. 263–274.

[18] L. CIARLETTA, M.-J. CHOI. *Autoconfiguration for VPN using Active XML*, in "5th International Workshop on IP Operations & Management - IPOM 2005, Barcelona, Spain", Oct 2005.

[19] L. CIARLETTA. *Emulating the Future with/of Pervasive Computing Research and Development*, in "What make for good application-led research, workshop Pervasive 2005, Munich, Germany", May 2005.

[20] L. CIARLETTA, C. HAMLAOUI. *Enabling autoconfiguration of the management plane using service discovery protocols*, in "International Conference of Computer Systems and Information Technology - ICSIT 2005, Algiers, Algeria", Jul 2005.

[21] V. CRIDLIG, H. ABDELNUR, J. BOURDELLON, R. STATE. *A NetConf Network Management Suite*, in "5th IEEE International Workshop on IP Operations & Management - IPOM 2005, Barcelona, Spain", Oct 2005.

[22] V. CRIDLIG, R. STATE, O. FESTOR. *An Integrated Security Framework for XML based Management*, in "9th IFIP/IEEE International Symposium on Integrated Network Management - IM 2005, Nice, France", A.

CLEMM, O. FESTOR, A. PRAS (editors). , May 2005, p. 587-600.

[23] V. CRIDLIG, R. STATE, O. FESTOR. *Architecture de sécurité fondée sur Radius pour le plan de gestion de réseau*, in "4ème Conférence sur la Sécurité et Architectures Réseaux - SAR 2005, Batz sur Mer, France", Jun 2005.

[24] V. CRIDLIG, R. STATE, O. FESTOR, J.-F. LEROY. *Radius-Based SNMP Authorization*, in "9th IFIP/IEEE International Symposium on Integrated Network Management - IM 2005 Application Session, Nice, France", May 2005.

[25] G. DOYEN, E. NATAF, O. FESTOR. *A hierarchical architecture for a distributed management of P2P networks and services*, in "16th IFIP/IEEE Distributed Systems : Operation and Management - DSOM'05, Barcelona, Spain", Oct 2005.

[26] G. DOYEN, E. NATAF, O. FESTOR. *Performance management of Distributed Hash Tables*, in "IFIP workshop on Networked Applications - EUNICE'05, Madrid, Espagne", Jul 2005.

[27] G. DOYEN, E. NATAF, O. FESTOR. *Une architecture hiérarchique pour une gestion distribuée des réseaux et services pair à pair*, in "Colloque Francophone sur la Gestion des Réseaux et Services - GRES 2005, Luchon, France", Feb 2005.

[28] A. LAHMADI, L. ANDREY, O. FESTOR. *On the Impact of Management on the Performance of a Managed System : A JMX-Based Management Case Study*, in "16th IFIP/IEEE International Workshop on Distributed Systems : Operations and Management - Management of Ambient Networks - DSOM 2005, Barcelona, Spain", J. S. JUERGEN SCHOENWAELDER (editor). , Lecture Notes in Computer Science, vol. 3775, Springer-Verlag, Oct 2005, p. 24–35.

[29] A. LAHMADI, L. ANDREY, O. FESTOR. *Performances et résistance au facteur d'échelle d'un agent de supervision basé sur JMX : Méthodologie et premiers résultats*, in "Colloque GRES 2005 : Gestion de REseaux et de Services, Luchon, France", A. BENZEKRI, M. SIBILLA (editors). , vol. 6, Mar 2005, p. 269-282.

[30] M. E. B. NASSAR, R. STATE, O. FESTOR. *Optimizing BGP confederation networks*, in "5th IEEE International Workshop on IP Operations and Management - IPOM 2005, Barcelona, Spain", Oct 2005.

Internal Reports

[31] H. ABDELNUR, R. STATE. *BGP Module Documentation for the PYenca Agent*, Technical report, Aug 2005.

[32] M. ADIB, A. BOUABDALLAH, M. S. BOUASSIDA, I. CHRISMENT, H. RAGAB, A. SERHROUCHNI. *L3.1 : Rapport sur l'analyse des algorithmes de cryptographie multicast*, Contrat, May 2005.

[33] L. ANDREY, A. LAHMADI, J. DELOVE. *A JMX benchmark*, Technical report, Nov 2005.

[34] R. BADONNEL, R. STATE, O. FESTOR. *Management of Ad-hoc Networks based on Probabilistic Guarantees*, Rapport de recherche, Apr 2005.

[35] R. Badonnel, R. State, O. Festor. *Using a Probabilistic Approach for Managing Ad-Hoc Networks*, Technical report, Jun 2005.

[36] R. Badonnel, R. State, O. Festor. *Using Information Theoric Measures for Detecting Faulty Behavior in Ad-Hoc Networks*, Technical report, Jun 2005.

[37] A. Bouabdallah, M. S. Bouassida, I. Chrisment, H. Ragab. *L3.2 : Etat de l'art des protocoles de gestion des clés dans les communications de groupe*, Contrat, May 2005.

[38] A. Bouabdallah, M. S. Bouassida, I. Chrisment, H. Ragab. *L3.3 : Définition d'un protocole de gestion de clé de groupe*, Contrat, May 2005.

[39] J. Bourdellon. *Conception et Implémentation d'un plan de gestion basé sur le protocole NetConf*, Technical report, Sep 2005.

[40] J. Braure. *Développement d'une infrastructure de supervision pour la plateforme JXTA*, Technical report, Sep 2005.

[41] T. Chown, M. Thompson, A. Ford, S. Venaas, C. Schild, C. Strauf, T. Kuefer, F. Beck, O. Festor, B. Gajda. *D3.6.1 : Cookbook for IPv6 Renumbering in SOHO and Backbone Networks*, Technical report, Jun 2005.

[42] N. Chridi, B. Fontan, S. Mota. *L2.5 SAFECAST : Spécification du système global - Intégration des services de sécurité au protocole de gestion de clés*, Technical report, Nov 2005.

[43] L. Ciarletta, O. Festor, R. State, F. Krief. *WP - 3.2.1 : Network Configuration*, Livrable 3.2.1 du projet RNRT SWAN, Rapport de contrat, Jan 2005.

[44] V. Cridlig, R. State. *YencaP Documentation*, Technical report, Jul 2005.

[45] X. Grandmougin. *Adaptation de l'architecture AAA aux réseaux ad hoc*, Technical report, Jun 2005.

[46] A. Lahmadi, L. Andrey, O. Festor. *Evaluation de performance des architectures de gestion de réseaux : état de l'art et perspectives*, Rapport de recherche, Jun 2005.

[47] A. Lahmadi, L. Andrey, O. Festor. *Extension des critères à la gestion par délégation : application à JMX & évaluation de l'approche*, Technical report, Nov 2005.

[48] A. Lahmadi, L. Andrey, O. Festor. *Synthèse et analyse des critères d'évaluation de performance des architectures de gestion*, Technical report, Nov 2005.

[49] M. E. B. Nassar. *Optimization des réseaux de confédérations basés BGP*, Technical report, Sep 2005.

Miscellaneous

[50] V. CRIDLIG, R. STATE, H. ABDELNUR, J. BOURDELLON, O. FESTOR. *EnSuite (Extended Netconf Suite)*, Nov 2005.

Bibliography in notes

[51] A.-L. BURNESS, R. TITMUSS, C. LEBRE, K. BROWN, A. BROOKLAND. *Scalability evaluation of a distributed agent system*, in "Distributed Systems Engineering", vol. 6, n^{o} 4, 1999, p. 129–134.

[52] E. CECCHET, J. MARGUERITE, W. ZWAENEPOEL. *Performance and Scalability of EJB Applications*, in "Proceedings of the 17th ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications", 2002, p. 246–261, http://rubis.objectweb.org/download/perf_scalability_ejb.pdf.

[53] P. JOGALEKAR, C. WOODSIDE. *Evaluating the scalability of distributed systems*, in "IEEE Transactions on Parallel Distributed. Systems", vol. 11, n^{o} 6, june 2000, p. 589–603.