



INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team MADYNES

*Management of Dynamic Networks and
Services*

Lorraine

THEME COM

Activity
R *eport*

2004

Table of contents

1. Team	1
2. Overall Objectives	1
3. Scientific Foundations	3
3.1. Evolutionary needs in network and service management	3
3.2. Autonomous management	3
3.2.1. Models and methods for a self-management plane	3
3.2.2. Integration of management information	4
3.2.3. Modelling and benchmarking of management infrastructures and activities	4
3.3. Functional Areas	5
3.3.1. Security: key management protocols and security of the management plane	5
3.3.2. Configuration: automation of service configuration and provisioning	6
3.3.3. Performance and availability monitoring	6
4. Application Domains	6
4.1. Mobile, Ad hoc and constrained networks	6
4.2. Dynamic Service Infrastructures	7
5. Software	7
5.1. MADYMAX: XML-based management for small devices	7
5.2. YENCA: configuration framework for IP networks	7
5.3. SSXG: secure XML/SNMP gateway	8
6. New Results	8
6.1. Securing the management plane	8
6.2. Secure Multicast in ad hoc networks	8
6.3. Management benchmarking	9
6.4. Management of peer-to-peer overlays	10
6.5. Monitoring and management of Ad Hoc networks	10
6.6. Autonomous management plane	10
7. Contracts and Grants with Industry	11
7.1. AMARILLO	11
7.2. SAFARI	12
7.3. SAFECAST	12
7.4. IST-6Net	13
7.5. MUSE	13
7.6. SWAN: Self aWare mAnagemeNt	14
8. Other Grants and Activities	14
8.1. International relationships and cooperations	14
8.2. National initiatives	15
8.3. Guest Researchers	15
9. Dissemination	15
9.1. Awards	15
9.2. Program committees and conference organisation	15
9.3. Teaching	16
9.4. Tutorials, invited talks, panels, presentations	16
9.5. Commissions	17
10. Bibliography	18

1. Team

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

This report covers the team activity from November, 1st 2003 to December 31st, 2004.

Team Leader

Olivier Festor [Research Director - INRIA]

Team Vice-Leader

Isabelle Chrisment [Assistant Professor, 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 [Assistant Professor, Nancy 2 University]

Laurent Ciarletta [Assistant Professor, ENSMN - Lorraine National Polytechnic Institute]

Jacques Guyard [Professor, ESIAL, Henri Poincaré - Nancy 1 University]

Emmanuel Nataf [Assistant Professor, Nancy 2 University]

André Schaff [Professor, ESIAL, Henri Poincaré - Nancy 1 University]

Project technical staff

Abelkader Lahmadi [INRIA, VTHD++ and 6Net contracts, until 31/10/2004]

Ph.D. Students

Rémi Badonnel [Industrial fund with regional co-sponsorship, 1st year]

Mohamed Salah Bouassida [MEN grant, 1st year]

Vincent Cridlig [Industrial fund with regional co-sponsorship, 1st year]

Guillaume Doyen [MEN grant, 2nd year]

Abelkader Lahmadi [Industrial fund, since 1/11/2004]

Hassen Sallay [ATER, Nancy 1 University, until august 31rd, 2004]

Post-doctoral Fellow

Mi-Jung Choi [Pohang University - Postech, Korea, since 1/10/2004]

Student Interns

Khalid Aid Abdelkrim [MS Degree Internship, ENSIAS, Morocco]

Adrien Bruneton [BS Degree Internship, ENST Paris, France]

Laurent Collet [BS Degree Internship, ESIAL, France]

Julien Delove [MS Degree Internship, DESS Informatique, University of Metz, France]

Marion Dugas [1st year Internship, INSA de Toulouse, France]

Chahinez Hamlaoui [MS Degree Internship, DEA Informatique, UHP - Nancy 1, France]

Oumina Hanane [MS Degree Internship, DEA Informatique, UHP - Nancy 1, France]

Adil El Kaisouni [MS Degree Internship, ENSIAS, Morocco]

Jean-Francois Leroy [BS Degree Internship, ESIAL, France]

Rizi Mohanti [BS Degree Internship, IIT-Kharagpur, India]

2. 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 team is to design, validate and deploy novel management and control paradigms as well as software architectures that are able to cope with the growing dynamicity and the scalability issues induced by the ubiquitous Internet.

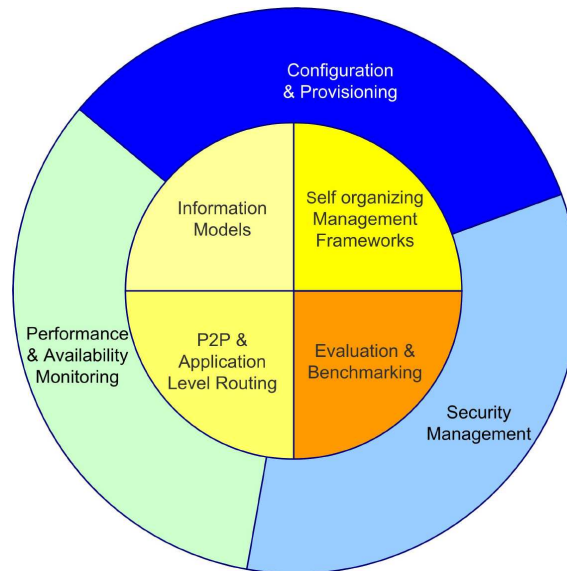


Figure 1. The MADYNES research themes

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.
- autonomous management is instantiated within **Functional Areas** (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 higher quality in the offered services. Because of its strategic importance and crucial interoperability requirements, 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 FCAPS¹ 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 to:

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

These three limits are observed in all five functional areas of the management domain 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 the standard functional areas: security, configuration and performance.

3.2. Autonomous management

3.2.1. Models and methods for a self-management plane

Self organisation and automation is a fundamental requirement 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 in several layers, like the IP auto-configuration or the 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 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 the locality or any other context information). So, this area represents a major challenge in extending current management approaches such 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.

¹Fault, Configuration, Accounting, Performance and Security

Design and evaluation of P2P-based management architectures Over the last years, several models 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 great 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 also have 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 environment rather than a standard centralised security framework).

Our approach envisions 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 using 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 forms a foundation of network and service management and remains an open research domain. The design and specification of new models is mainly driven by the emergence 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 for the problem of the modelling and representation of management information aims to:

1. enable 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. foster the use of standard models (at least the structure and semantics of well defined models),
3. design a naming structure that allows the routing of management information in an overlay management plane, and
4. evaluate 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 highly depends on three factors:

- the distribution of the considered service and the 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 an objective evaluation of operational cost 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 in battery and processing limited devices or in bandwidth limited wireless networks for which the lack of a management cost models is a serious concern.

MADYNES addresses this problem from multiple viewpoints: communication, patterns and processing and/or 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 activity.

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 which 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 that needs to be undertaken in this activity is the design and 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 points:

1. Abstraction of the various access control mechanisms that exist in today’s management frameworks. We are particularly interested in extending these models so that they support event-driven management which is not the case in most of them today.
2. Extension of policy and trust models to ease and 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 envisioned 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 offer proprietary interfaces and protocols for their use.

These two basic limits highly impact 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 of either a service, a device or a network configuration and to associate to this model a generic command and programming interface. This is done in a way similar to what is followed 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 their 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 underlies almost any service, and becomes crucial for any service which is bound to a service level agreement describing the expected service delivery level. Performance management needs models, metrics, associated instrumentation, data collection and aggregation infrastructures as well as 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 and offers an API enabling application developers to easily integrate measurement within their distributed application. While this approach is very interesting, it is only a first step in 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 as well as 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 that emerge 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 key distribution, monitoring and accounting. 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) and/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 and,
- peer-to-peer infrastructures.

5. Software

5.1. MADYMAX: XML-based management for small devices

Participants: Olivier Festor, Radu State [Correspondent].

MADYMAX is a management toolkit for **SyncML**-based device management.

The framework provides the necessary libraries and tools to automate the development of management agents for the SyncML device management framework and offers rich management data transport capabilities. Based on user-specified management interfaces, management agents can be extended to support new management objects. This extension can be done at run-time (in case of Java based service management), or at compile-time (in case of device specific native management).

The toolkit is registered within the APP and is freely distributed under an open source (LGPL) license. It is available on the team's web site(<http://madynes.loria.fr>). The framework together with a performance study of its protocols and operations was presented in [21].

5.2. YENCA: configuration framework for IP networks

Participants: Olivier Festor, Radu State [Correspondent].

YENCA is an XML based network management framework compatible with the draft IETF NetConf specification. Its aim is to offer the community a development package for NetConf based configuration management of networked devices.

YENCA provides following features:

- a full implementation of the NetConf protocol (both in Java and C),
- a basic NetConf Agent (written in C) for IPv4/IPv6 interface management,
- support for modular agent extension,
- a simple Java GUI for the manager.

The toolkit is registered within the APP and is freely distributed under an open source (GPL) license. It is available on the team's web [site](#) and is registered as a sourceforge project. YENCA is currently evaluated within several universities and companies. The project has a critical mass of contributors and several new modules are currently under development in several teams around the world.

5.3. SSXG: secure XML/SNMP gateway

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

SSXG is a secure XML/SNMP gateway. Based on an initial gateway developed at the University of Braunschweig in Germany by Frank Strauss and Torsten Klie, it allows network administrators to manage SNMP agents through a web interface and XML in a secure way.

SSXG extends the initial gateway through:

- an embedded Role-Based Access Control model (RBAC),
- an access control configuration and security configuration engine,
- full support of the Simple Network Management Protocol v3 User Security Model (USM) and View-based Access Control Model (VACM).

SSXG is registered as a sourceforge project. Due to several external requests, the SNMP VACM/USM configuration engine is currently under investigation to become a standalone distribution.

6. New Results

6.1. Securing the management plane

Participants: Laurent Collet, Vincent Cridlig, Olivier Festor, Jean-François Leroy, Radu State [Correspondent].

Securing the management plane is one of the main research activities of our group. 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 multiple managed devices and dynamic manager to-agent interaction and (2) providing a good and uniform security independently of the management interface/protocol.

Our research activity focuses on providing a uniform security continuum independent on the underlying management protocol and interface. Our first contribution addresses the case of an XML/SNMP management plane, where XML/SNMP based managers interact with SNMP devices. We have defined a flexible RBAC enabled access control plane, capable to mediate the manager-to-agent interaction. We have also defined a mapping from the XML-specified RBAC module to the SNMP standardized access control module (VACM). This work has been presented at the IEEE/IFIP DSOM 2004 symposium [15] and has been awarded by the best student paper award. An implementation of the framework has been made and is distributed as part of the SSXG framework [29].

We extended this work to a more general case of highly dynamic XML based management plane. Our approach [30] proposes an integrated security framework for the NetCONF protocol. NetConf is the XML based protocol standard for network management currently under standardization within IETF. We proposed a security framework integrating confidentiality, authentication and access control within a higher conceptual distributed RBAC model [30]. Scalability is addressed by efficient large group key distribution, where a multicast group is the logical equivalent of devices and role endorsed by multiple managers.

6.2. Secure Multicast in ad hoc networks

Participants: Mohamed Salah Bouassida, Adrien Bruneton, Isabelle Chrisment [Correspondent], Olivier Festor, Abdelkader Lahmadi.

We are working on the design of security and key distribution protocols that satisfy the strong constraints imposed by the combination of ad-hoc networks and multicast communications.

In 2004, we studied the authentication issue in ad hoc environment. We defined a classification of the authentication approaches dedicated to group communications and more specifically those related to source authentication. We also evaluated their adequacy in the context of ad-hoc networks [13][26].

The study of authentication schemes was completed with a survey on group key management services for group communications in ad hoc environment [27]. This study has led to the establishment of a tutorial [11] concerning security and group communication. This tutorial was given at the ING 2004 summer school by Isabelle Chrisment together with Professor Bouabdallah from the technology University of Compiègne.

Traditional group key management architectures proposed for wired networks are not appropriate in ad hoc environment, mainly due to their high dynamicity and the mobility of nodes. We defined an enhanced hybrid key management protocol for secure multicast dedicated to operate in ad hoc networks [12]. Built on a protocol called BAAL [42] which is dedicated to key distribution in wired networks, the approach integrates threshold cryptography [44] combined with the services of the AKMP [41] protocol. This combination enables the fast delivery and efficient key distribution in a multicast service. This work was also presented during the student session, in the summer school, **ING 2004**.

This proposal has been extended to cope with mobility-aware key management for multicast services, in which the sources follow each other in a sequential way (1 towards N sequential model). In this context, we designed a new protocol of group key management we called BALADE [28]. The efficiency of our model is validated by analysis and its applicability is illustrated through its implementation in a distributed cooperative juke-box environment currently under development in the team.

We are now working on the establishment of an efficient clustering scheme for multicast key distribution in mobile ad hoc networks based on the localization of the group members and their mobility. Our objective is to integrate this clustering scheme in the BALADE protocol.

6.3. Management benchmarking

Participants: Laurent Andrey [Correspondent], Julien Delove, Olivier Festor, Abdelkader Lahmadi, Hanane Oumina.

In 2004, we investigated two issues in the area of management benchmarking, namely the performance of JMX-based management and the evaluation of the impact of security on SNMPv3 performance.

The work on JMX resulted in the definition of a test suite for JMX-based management frameworks. This test suite is a “synthetic micro-test” to inject a basic JMX traffic (get request to read a management attribute) according to various tests factors. The main test factors are:

- JMX support, i.e. we currently support in the test process the Sun reference implementation as well as 2 open sources implementations (MX4J, JBOSS-MX),
- injection rate expressed as “number of get requests per second”,
- numbers of MBeans (managed objects) located in the agent side,
- number of attributes exposed by various MBeans.

The metrics used for this micro-tests service are simple: memory usage, CPU consumption, bandwidth consumption and number of correct `get` and `get-requests` completed per second. This suite has been packaged to be easily used by the community [31].

In the context of SNMP performance measurement, we conducted an initial study on the impact of the Simple Network Management Protocol v3 security mechanisms on performances [33]. First, We performed basic benchmarking to calibrate the parameters of the planed simulation. This simulation shows that the overload generated by User Based Security (USM) is low enough (less than 10 % of processor resource and small impact on SNMP message size) to keep the polling scheme usable between one manager and a large number of agents.

6.4. Management of peer-to-peer overlays

Participants: Guillaume Doyen, Olivier Festor [Correspondent], Rizzi Mohanti, Emmanuel Nataf.

Based on the evaluation of common components in P2P systems, we have designed a generic management information model for P2P networks and services. Our model aims at providing an abstract view of a P2P network to a manager. This view includes: the enumeration of participating elements, the virtual topology and organisation, the amount of available resources, communication elements and services [16]. The model is specified as an extension of the Common Information Model (CIM) which is a standard information model for management developed within the Distributed Management Task Force (DMFT) and which offers a good set of abstraction for the management of distributed systems and applications.

To validate our information model, we did instantiate it on two different P2P infrastructures, namely *Jxta* and *Chord* [43]. *Jxta* is a generic framework dedicated to the development of P2P applications and services. We have fully instrumented a *Jxta* peer and integrated the management data into a JMX agent [37]. Thereby, we are able to monitor a *Jxta* peer. *Chord* is a well known Distributed Hash Table (DHT)-based P2P infrastructure.

A second contribution was the abstraction of our work on *Chord* towards performance management of distributed hash tables (DHT) in general. Today, DHTs are the core of many other P2P applications and frameworks and they provide reliable routing and discovery functionalities. To illustrate the specialization we performed on the model, we have designed the information model for the *Chord* framework. Therefore, we have designed the performance metrics that concern the dynamics of the DHT, namely:

- the resources balancing among the participants,
- the average path length, and
- the metadata consistency.

Then, we have integrated these metrics in a refinement of our information model dedicated to the performance monitoring of DHTs [18].

We are now working on the deployment issues of our model in a P2P environment, and especially the concept of a P2P manager and the distribution of the management data.

6.5. Monitoring and management of Ad Hoc networks

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

The monitoring of ad-hoc networks is a particularly important and challenging research issue done in our group. The major challenges consist in researching both a well defined set of parameters to be monitored as well as an underlying monitoring architecture.

We have designed an end to end connectivity measure for ad-hoc networks and performed an extensive set of experimental analysis of this measure with respect to specific parameters: mobility model, network size, and deployment surface [25].

Our results can be easily used for static network provisioning and as building blocks for a monitoring framework. Our work towards the latter, is summarized in [23] where we propose a management architecture, capable to provide dynamic configuration of the routing plane for an ad-hoc network. This work is extended with a complete information model, an OLSR Management Information Base and associated traffic monitoring algorithms [24].

Work on the management of ad-hoc networks towards a policy based management framework was also continued partly in cooperation with the ARES research group located at INRIA Rhône-Alpes. The resulting management architecture was published in [14].

6.6. Autonomous management plane

Participants: Laurent Ciarletta, Chahinez Hamlaoui, Adil El Kaysouni, Olivier Festor [Correspondent], Radu State.

With the growing number of entities in the management plane and their overall dynamics, there is a strong need for automatic configuration (as opposed to manual configuration done by network administrators).

In 2004, we investigated the use of service discovery protocols [34] to configure both agents and managers in an automated way. Our solution is based on multicast DNS and DNS SD (Service Discovery) developed in the IETF Zeroconf Working Group. With these protocols, discovery and configuration of agents and managers are automatically done. In our case, agents and managers are providing services, and we are configuring SNMP entities. An agent needs to find a suitable manager that can deal with its properties, while managers discover agents that they can manage in return. This solution can be extended to automatic reconfiguration of the management plane.

Following our work on using P2P architectures for Web-based (XML) management, we looked into the use of **Active-XML**, to configure IPsec tunnels (VPN endpoints). Active-XML is a P2P Web Service architecture where Active-XML documents are themselves XML documents that embed calls to Web Services. In the frame of the SWAN project, we developed a model and a prototype [32] that allows for the automatic generation of IPsec parameters (XML configuration documents) when 2 or more domains want to establish secured communication channels. Active-XML Web Services are dynamically exchanging basic security requirements and capabilities and are negotiating the configuration parameters. The Active-XML documents are then configuring the IPsec parameters. Our prototype can also provide feed-back from the actual tunnels.

7. Contracts and Grants with Industry

7.1. AMARILLO

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

Dates December 2003 - January 2006

Partners Thalès (leader), INRIA-MADYNES, LIP6, ENST, Paris XIII University.

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

The MADYNES contributions to this project are:

- a study on management benchmarking and the evaluation 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.

7.2. SAFARI

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

Dates February 2003 - January 2006

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

SAFARI is an French National Research in Telecommunications (RNRT) agency funded precompetitive research project. The goal of the project is to design, setup and 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 team.

7.3. SAFECAST

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

Dates March 2004 - March 2007

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

SAFECAST is a French National Research in Telecommunications (RNRT) agency funded research project. 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 or and a receiver. The security of group communication will have to be provided while allowing dynamicity of receivers. Each receiver can join ou 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 team.

7.4. IST-6Net

Participants: Olivier Festor [Correspondent], Abdelkader Lahmadi.

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 topology discovery algorithm for IPv6 Local Area Networks. We implemented the IPv6 MIB-2 on the net-snmp framework and ported several environments on IPv6 (NAGIOS, NTOP, Looking glass services).

Since december 1st, 2004, MADYNES is contributing to a new action within 6Net, namely network renumbering. Our activity on this action, is to evaluate the impact of network renumbering on the management plane itself.

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

7.5. MUSE

Participant: Olivier Festor [Correspondent].

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 team is contributing to the project under the leadership of Stéphane Frénot from the ARES team 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.

7.6. SWAN: Self aWare mAnagemeNt

Participants: Laurent Ciarletta [Correspondent], 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 his goals, the project identified 3 key working areas:

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

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.

We maintain an informal cooperation with the team 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 2004, we participated to three NMRG meetings (Bremen in January, Seoul in May and Davis in November).

Aiko Pras will co-chair with Olivier Festor and Alexander Clemm the IFIP/IEEE International Symposium on Integrated Network Management in 2005. Olivier Festor together with Aiko Pras and Juergen Schönwälder co-edited a special issue of IEEE Communications Magazine on XML-based management in July 2004.

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.

We hosted students from the ENSIAS engineering school in Morocco (ENSIAS) for their master thesis degree training period. We did also host one student from the Indian Institute of Technology for his bachelor's degree training period.

MADYNES is also an active member of the STIC-Asia initiative which promotes cooperation between France and several Asian countries and 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.

8.2. National initiatives

In addition to the cooperation with the various partners within national funded 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 CNRS summer school which was held in Obernai in June 2004 and the team is regularly contributing to the organization of the school and is a contributor to several tutorials given during the school week.

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

MADYNES, through Laurent Andrey is contributing to the CNRS funded specific action called OSS-CR which is a group of researchers who are interested in the monitoring and management of large scale systems.

8.3. Guest Researchers

Since October 2004, Mi-Jung Choi has joined the MADYNES team 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 is working on the extension of the YENCA netconf environment towards IPv6 firewalling configuration support and she will continue the investigation on the use of XML-based techniques for autonomous management and their application to VPN management.

9. Dissemination

9.1. Awards

Vincent Cridlig received the “Best Student Paper Award” at the IFIP/IEEE DSOM 2004 event for the paper entitled “Role-Based Access Control for XML Enabled Management Gateways” co-authored with Radu State and Olivier Festor.

9.2. Program committees and conference organisation

Isabelle Chrisment was member of the program committee of the following events: SAR 2004 and NOTERE 2004.

Radu State was member of the program committee of SAR 2004 and IFIP/IEEE DSOM 2004. He was member of the JDIR 2004 Technical Program Committee. He is also reviewer for several major journals and conferences for the ACM. He chaired the short papers session at DSOM 2004.

In 2004, Olivier Festor was member of the following program committees: IFIP/IEEE Distributed Systems: Operations and Management (DSOM 2004), IFIP/IEEE Network Operation and Management Symposium (NOMS 2004), ING 2004 Summer school, Des Nouvelles Architectures de Communication (DNAC 2004), NOTERE 2004.

Olivier Festor is also member of the Board of Editors of the Journal of Systems and Network Management and reviewed 48 papers for several international conferences and journals in 2004. He served as an expert in telecommunications for the “Fond de recherche sur la nature et les technologies” from the Québec Government and the “National Sciences and Engineering Research Council of Canada”. He also served as an expert reviewer for the European Commission in the context of the 6th Framework. Olivier Festor chaired the session entitled ‘Management Architectures at DSOM 2004 and the session on “Information Models” at NOMS 2004.

André Schaff was member of the NOTERE 2004 technical program committee.

9.3. 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 assistant 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 DEA degree, TRS (Telecommunications, Networks and Services) specialisation, Isabelle Christment is in charge of the course entitled *Advanced Internet Protocols*; Olivier Festor is in charge of the course entitled OVERLAY NETWORKS AND SERVICE INFRASTRUCTURES This course is shared with Pr. Francis Lepage (CRAN).

Isabelle Christment is heading the Telecommunications and Networks specialisation of the 3rd year at the ESIAL² 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 is co-leader of the Distributed Services and Communication Networks Research specialization of the new Masters of Computer Science proposal for the Universities in Lorraine.

André Schaff is the Director of the ESIAL Engineering School.

Laurent Andrey is the head of computer science departement at the IUT in Verdun.

9.4. Tutorials, invited talks, panels, presentations

In 2004, Olivier Festor and André Schaff co-edited a book providing the state of the art in network and Service Management [2]. 4 chapters of the book were authored by members of the MADYNES team [9][8][7][6].

Olivier Festor was invited as a panelist at the IFIP/IEEE DSOM'2003 event in Heidelberg, Germany in October 2003. The panel topic was "Self-managing distributed systems".

Isabelle Christment and Pr. Bouabdallah gave a tutorial on multicast security at the Next Generation Internet (ING) summer school in June 2004.

Olivier Festor and Radu State gave a tutorial on configuration management at the Next Generation Internet (ING) summer school in June 2004.

Radu State gave a short tutorial on network security and attacks at the SAR 2004 conference in June 2004. He gave a talk on SyncML at the IRTF NMRG meeting in Bremen, January 2004, and made a presentation of the YENCA toolkit at the Seoul meeting of the NMRG.

Guillaume Doyen gave a presentation at the SAFARI workshop, held in conjunction with the Sixth IFIP IEEE International Conference on Mobile and Wireless Communication Networks in Paris on October 2004.

Guillaume Doyen gave a presentation on the JXTA Framework and a presentation on P2P management at the GERET symposium held in Nancy on 25-28 March 2004.

Olivier Festor presented the MADYNES vision of autonomous management to the ILOG scientific board in 2004.

Mohamed Salah Bouassida and Vincent Cridlig both presented their research results as part of the Ph.D. Student track of the Next Generation Internet (ING) summer school in June 2004.

Vincent Cridlig gave an invited presentation on the security of the management plane at the SAR conference in June 2004.

The multiple project and collaboration meetings have also seen participation from one or several members of the MADYNES Team. For all conferences in which a paper from the team was published, a team member attended and presented the work.

²Ecole d'Ingénieurs en Informatique et ses Applications de Lorraine

9.5. Commissions

Olivier Festor is member of the SPECIF Ph.D. Award Jury which awards every year the best Ph.D. in computer science in France.

Following Ph.D. defenses were held by members of the team :

- Hassen Sallay, Ph.D. in Computer Science from the Henri Poincaré University Nancy 1, France. Title *Architecture de supervision et modèle de comptabilité pour le Multicast IP*. Committee : Rachida Dssoulli (rapporteur), Olivier Festor (co-directeur de thèse), Jacques Jaray, Pascale Primet (rapporteur), André Schaff (co-directeur de thèse), March 2004.
- Mouna Benaissa Ph.D. in Computer Science from the Henri Poincaré University Nancy 1, France. Title *Ajustement dynamique du délai de présentation des paquets pour le transport de la voix dans les réseaux ad hoc*. Committee: Andrzej Duda (rapporteur), Jean-Pierre Elloy (rapporteur), Frédéric Alexandre, Vincent Lecuire, Francis Lepage (co-directeur de thèse), André Schaff (co-directeur de thèse), February 2004.

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

- Hoa-Binh Nguyen., Ph.D. in Computer Science from the National Polytechnic Institute of Grenoble, *Services Actifs et Passerelles Programmables - Active Services and Programmable Gateways*. Committee: Ken Chen (rapporteur), Andrzej Duda (directeur de thèse), Olivier Festor (rapporteur), Yvon Gourhant, Brigitte Plateau, February 2004.
- Olivier Corre, Ph.D. in Computer Science from the Pierre et Marie Curie University - Paris 6, France. Title *Gestion dynamique de services par politiques dans un réseau d'opérateur de télécommunications*. Committee : Olivier Festor (rapporteur), Jean-Philippe Martin-Flatin (rapporteur), Nazim Agoulmine, Mickael Salaun, Patrick Cocquet, December 2004.
- Christophe Jelger, Ph.D. in Computer Science from the Louis Pasteur University of Strasbourg, France. Title *Gestion des équipements mobiles et communications de groupe dans l'Internet Nouvelle Génération*. Committee: Philippe Clauss (rapporteur), Olivier Festor (rapporteur), Eric Fleury, Thomas Noël (co-directeur de thèse), Jean-Jacques Pansiot (co-directeur de thèse), Guy Pujolle (rapporteur), October 2004.
- Emmanuel Reuter, Ph.D. in Computer Science from Nice-Sophia Antipolis University, Title *Agents Mobiles: itinéraires pour l'administration système et réseau*, Committee: Françoise Baude (directeur de thèse), Serge Chaumette, Olivier Festor (rapporteur), Michel Riveill (rapporteur), May 2004.

MADYNES members were members of the following Habilitation Degree commission:

- Thomas Noël, HDR from Louis Pasteur University - Strasbourg, France; Title: *Communications de Groupe: du parallélisme au ad hoc*, Commission: Andrzej Duda, Serge Fdida (rapporteur), Philippe Jacquey (rapporteur), Stéphane Ubéda, Olivier Festor (rapporteur) december 2003.
- Michèle Sibilla, HDR from Paul Sabatier University - Toulouse, France ; Title: *Gestion de systèmes complexes: Un cadre complet conduit par des modèles objets PI/PS*, Commission: Nazim Agoulmine (rapporteur), Jean Bézivin, Olivier Festor (rapporteur), Yves Raynaud, Michel Riveill (rapporteur), Noémie Simoni, december 2004.

Isabelle Chrisment was an elected member of the hiring committee in Computer Science at the Henri Poincaré - Nancy 1 University (27th section) and a nominated member at the Louis Pasteur University in Strasbourg.

Since october 2004, Olivier Festor is a nominated member of the hiring committee in Computer Science at the Louis Pasteur University in Strasbourg since October 2004. He is also 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 in Computer Science.

10. Bibliography

Books and Monographs

- [1] O. FESTOR, A. PRAS, J. SCHÖNWÄLDER. *IEEE Communications Magazine - Special issue on XML-Based Management of Networks and Services*, IEEE Communications Magazine, vol. 42, n° 7, IEEE, July 2004.
- [2] O. FESTOR, A. SCHAFF. *Standards pour la gestion des réseaux et des services*, IC2 Réseaux et Télécoms, Hermès Science Publishing, January 2004.

Doctoral dissertations and Habilitation theses

- [3] M. BENAÏSSA. *Ajustement dynamique du délai de présentation des paquets pour le transport de la voix dans les réseaux ad hoc*, Thèse d'université, UHP Nancy 1, April 2004.
- [4] H. SALLAY. *Architecture de supervision et modèle de comptabilité pour le Multicast IP*, Thèse d'université, UHP, February 2004.

Articles in referred journals and book chapters

- [5] G. CHADDOUD, V. VARADHARAJAN, I. CHRISMENT, A. SCHAFF. *Gestion efficace de la sécurité des communications de groupe pour le service SSM*, in "RSTI-TSI", vol. 23, n° 9, December 2004, p. 1107-1135.
- [6] O. FESTOR, L. ANDREY. *JMX : un standard pour la gestion Java*, in "Standards pour la gestion des réseaux et des services", A. S. OLIVIER FESTOR (editor)., IC2 Réseaux et Télécoms, chap. 6, Hermès Science Publishing, January 2004, p. 213-250.
- [7] O. FESTOR, N. BEN YOUSSEF. *L'initiative WBEM*, in "Standards pour la gestion des réseaux et des services", A. S. OLIVIER FESTOR (editor)., IC2 Réseaux et Télécoms, chap. 5, Hermès Science Publishing, January 2004, p. 159-212.
- [8] O. FESTOR, N. BEN YOUSSEF. *Le modèle CIM*, in "Standards pour la gestion des réseaux et des services", A. S. OLIVIER FESTOR (editor)., IC2 Réseaux et Télécoms, chap. 4, Hermès Science Publishing, January 2004, p. 113-157.

- [9] E. NATAF. *La gestion distribuée avec SNMP - l'approche DISMAN* -, in "Standards pour la gestion des réseaux et des services", A. S. OLIVIER FESTOR (editor), IC2 Réseaux et Télécoms, chap. 2, Hermès Science Publishing, January 2004, p. 37-75.

Publications in Conferences and Workshops

- [10] R. BADONNEL, L. ANDREY, O. FESTOR. *Architecture pour la gestion de la qualité de service dans les services Web, reposant sur une extension d'un langage de composition*, in "Les Nouvelles Technologies de la RÉpartition - NOTERE'04, Saidia, Maroc", R. Dssouli, F. Khendek and A. Serhrouchni, June 2004.
- [11] A. BOUABDALLAH, I. CHRISMENT. *IP Multicast Security*, in "Ecole d'été Internet Nouvelle Génération RHDM-ING, Obernai, France", CNRS, June 2004, <http://www.loria.fr/publications/2004/A04-R-228/A04-R-228.ps>.
- [12] 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, Athènes, Grèce", N. MITROU, K. KONTOVASILIS, G. ROUSKAS (editors), Lecture Notes in Computer Science, vol. 3042, Springer-Verlag, May 2004, p. 725-742.
- [13] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *Méthodes d'Authentification pour les Communications de Groupes : Taxonomie et Evaluation dans un environnement Ad Hoc*, in "3ème Conférence sur la Sécurité et Architectures Réseaux - SAR'2004, La Londe, Côte d'Azur, France", June 2004, p. 197-208, <http://www.loria.fr/publications/2004/A04-R-096/A04-R-096.ps>.
- [14] C. CHAUDET, O. FESTOR, I. GUÉRIN LASSOUS, R. STATE. *A Managed Bandwidth Reservation Protocol for Ad Hoc Networks*, in "First International Workshop on Service Assurance with Partial and Intermittent Resources - SAPIR 2004, Fortaleza, Brazil", P. DINI, P. LORENZ, J. N. DE SOUZA (editors), Lecture Notes in Computer Science, vol. 3126, Springer, August 2004, p. 13-20.
- [15] 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, November 2004, p. 183-195.
- [16] G. DOYEN, O. FESTOR, E. NATAF. *A CIM Extension for Peer-to-Peer Network and Service Management*, in "11th International Conference on Telecommunications - ICT'2004, Fortaleza, Brésil", J. N. DE SOUZA, P. DINI, P. LORENZ (editors), Lecture notes in Computer Science, vol. 3124, Springer, August 2004, p. 801-810.
- [17] G. DOYEN, O. FESTOR, E. NATAF. *JXTA : une infrastructure générique pour le développement d'applications P2P*, in "Groupe d'Exploitation des Réseaux Ethernet TCP/IP - GERET, Nancy, France", March 2004, <http://www.loria.fr/publications/2004/A04-R-519/A04-R-519.ps>.
- [18] G. DOYEN, E. NATAF, O. FESTOR. *A Performance-Oriented Management Information Model for the Chord Peer-to-Peer Framework*, in "IFIP/IEEE International Conference on Management of Multimedia Networks and Services - MMNS'2004, San Diego, Californie, USA", J. VICENTE, D. HUTCHISON (editors), Lecture notes in Computer Science, vol. 3271, Springer, October 2004, p. 200-212.

- [19] O. FESTOR, R. STATE. *Gestion de configuration : Modèles, Langages, Protocoles et Usages*, in "Ecole d'été Internet Nouvelle Génération RHDM-ING, Obernai, France", CNRS, June 2004, <http://www.loria.fr/publications/2004/A04-R-137/A04-R-137.ps>.
- [20] A. KELLER, R. BADONNEL. *Automating the Provisioning of Application Services with the BPEL4WS Workflow Language*, 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, November 2004, p. 15-27.
- [21] R. STATE, O. FESTOR, B. ZORES. *An extensible Agent Toolkit for Device Management*, in "10th IEEE/IFIP Network Operations and Management Symposium - NOMS'2004, Seoul, Korea", R. BOUTABA, S.-B. KIM (editors)., IEEE Press, April 2004, p. 845-858.

Internal Reports

- [22] K. AIT ABDELKRIM. *Management of OSGi Home Gateway*, Projet de Fin d'Etude, April 2004.
- [23] R. BADONNEL, R. STATE, O. FESTOR. *A Management Framework for Coverage in Mobile Ad-Hoc Networks*, Rapport de recherche, June 2004.
- [24] R. BADONNEL, R. STATE, O. FESTOR. *Management of Mobile Ad-hoc Networks : Evaluating the Network Behavior*, Rapport de recherche, July 2004.
- [25] R. BADONNEL, R. STATE, O. FESTOR. *Monitoring Coverage In Dynamic Wireless Ad-Hoc Networks*, Rapport de recherche, February 2004.
- [26] A. BOUABDALLAH, M. S. BOUASSIDA, Y. CHALLAL, I. CHRISMENT. *Etat de l'art des protocoles d'authentification dans les communications de groupe*, Rapport intermédiaire du projet SAFECAS, October 2004.
- [27] M. S. BOUASSIDA, I. CHRISMENT, V. GUYOT, V. LEGRAND, D. RAFFO, S. UBEDA. *L4.02 : Sécurité et Réseaux Ad Hoc*, Rapport intermédiaire du projet SAFECAS, April 2004.
- [28] M. S. BOUASSIDA, A. LAHMADI, I. CHRISMENT, O. FESTOR. *Diffusion multicast sécurisée dans un environnement Ad-Hoc (1 vers n séquentiel)*, Rapport de recherche, INRIA, September 2004, <http://www.inria.fr/rrrt/rr-5310.html>.
- [29] L. COLLET, V. CRIDLIG. *Sécurisation d'une Passerelle XML - SNMP*, Stage 2ème année ESIAL, September 2004, <http://www.inria.fr/rrrt/rr-5310.html>.
- [30] V. CRIDLIG, R. STATE, O. FESTOR. *Secure XML-based Network Management in a Multi-source Context*, Rapport de recherche, July 2004, <http://www.loria.fr/publications/2004/A04-R-080/A04-R-080.ps>.
- [31] J. DELOVE. *Tests de performance et JMX*, Stage de DESS de l'Université de Metz, September 2004.

- [32] A. EL KAYSOUNI. *Auto-configuration des VPNs - IPSec*, stage ingénieur, ENSIAS, June 2004, <http://www.loria.fr/publications/2004/A04-R-142/A04-R-142.ps>.
- [33] H. EZ-ZAHRA OUMINA. *L'évaluation du modèle gestion/agent dans la gestion de réseaux et services*, Stage de DEA, Loria-UHP, June 2004, <http://www.loria.fr/publications/2004/A04-R-466/A04-R-466.ps>.
- [34] C. HAMLAOUI. *Exploitation des protocoles de découverte de services pour l'auto-configuration du plan de gestion*, Stage de DEA, June 2004, <http://www.loria.fr/publications/2004/A04-R-143/A04-R-143.ps>.
- [35] A. LAHMADI, O. FESTOR. *Extension of a network monitoring tool with IPv6 features (Ntop)*, Rapport technique, February 2004, <http://www.inria.fr/rrrt/rt-0292.html>.
- [36] J.-F. LEROY, V. CRIDLIG. *RADIUS-Based SNMP Authorisation*, Stage 2ème année ESIAL, September 2004.
- [37] R. MOHANTY. *Instrumentation of the Jxta peer-to-peer framework*, Stage d'école d'ingénieur (2ème année), September 2004, <http://www.loria.fr/publications/2004/A04-R-471/A04-R-471.ps>.
- [38] H. OUMINA, R. STATE, O. FESTOR, C. CHAUDE, I. GUÉRIN LASSOUS. *L2.03 : Interfaçage d'un protocole de QoS avec l'architecture de gestion de QoS du sous-projet 4 du projet RNRT SAFARI*, Rapport intermédiaire du projet SAFARI, January 2004.

Miscellaneous

- [39] R. STATE. *Cours Sécurité Réseaux*, Notes du cours sur la détection d'intrusion et les attaques dans l'Internet dispensé à l'ESIAL, March 2004.
- [40] R. STATE. *Exploring Security*, Invited talk given at SAR'2004, January 2004.

Bibliography in notes

- [41] H. BETTAHAR, A. BOUABDALLAH, Y. CHALLAL. *An Adaptive Key Management Protocol for Secure Multicast*, in "Proceedings of the 11th IEEE-International Conference on Computer Communications and Networks ICCCN'02, Miami, Florida, USA", October 2002, p. 125-133.
- [42] G. CHADDOUD. *Sécurisation de communication de groupes dynamiques*, Thèse d'université, Université Henri Poincaré, Aug 2002.
- [43] I. STOICA, R. MORRIS, D. KARGER, M. F. KAASHOEK, H. BALAKRISHNAN. *Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications*, in "Proceedings of the ACM SIGCOMM '01 Conference, San Diego, California", August 2001.
- [44] L. ZHOU, J. HAAS. *Securing Ad Hoc Networks*, in "IEEE Network", vol. 13, n° 6, 1999, p. 24-30, <http://citeseer.nj.nec.com/zhou99securing.html>.