INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Madynes

Management of Dynamic Networks and Services

Lorraine

THEME COM

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 and publications from December, 1st 2005 to December 31th, 2006.

Head of the team

Olivier Festor [Research Director (DR) INRIA, HdR]

Vice-head of the team

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

Administrative Assistant

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

INRIA Staff

Radu State [Researcher Associate (CR) 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, HdR]
Emmanuel Nataf [Associate Professor, Nancy 2 University]
André Schaff [Professor, ESIAL, Henri Poincaré - Nancy 1 University, HdR]
Guillaume Doyen [ATER, Henri Poincaré - Nancy 1 University. Until September 2006]

Project Technical Staff

Frédéric Beck [Engineer, Industrial grant]
Balamurugan Karpagavinayagam [Engineer, INRIA associate engineer program (since 09/2006)]

Ph.D. Students

Rémi Badonnel [Industrial grant with regional co-sponsorship, 3rd year]
Mohamed Salah Bouassida [MEN grant, 3rd year]
Vincent Cridlig [Industrial grant with regional co-sponsorship, 3rd year]
Abelkader Lahmadi [Industrial grant, 2nd year]
Mohamed Nassar [MEN grant, 1st year]
Humberto Jorge Abdelnur [Industrial grant with regional co-sponsorship, 1st year]

Student Interns

Jérôme François [MS Degree Internship, DEA Informatique, Henri Poincaré - Nancy 1 University]
Christophe Levointurier [MS Degree Internship, DEA Informatique, Henri Poincaré - Nancy 1 University]
Mahamed Bouali [MS Degree Internship, DEA Informatique, Technical University of Compiègne]
Christi Poppi [Ms Degree Internship, University of Timişoara, Roumania]
Mathieu Colonna [2nd year internship, engineering school, ESIAL Henri Poincaré - Nancy 1 University]
Thibault Cholez [2nd year internship, engineering school, ESIAL, Henri Poincaré - Nancy 1 University]
Anca Ghitescu [Ms Degree Internship, Technical University Hamburg-Harburg, Germany]

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*.

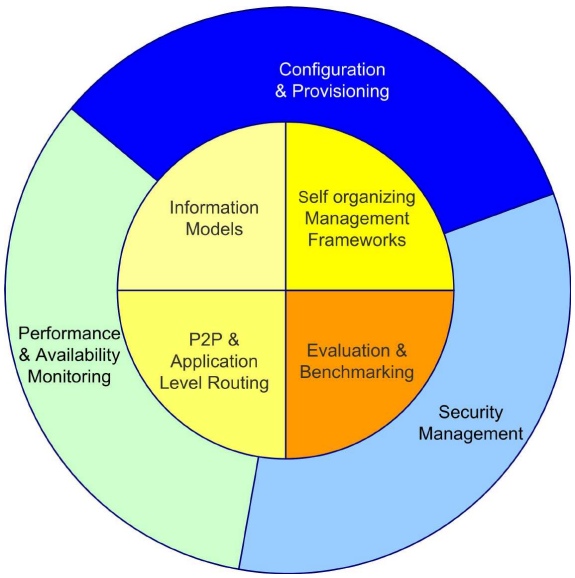

Figure 1. The MADYNES research themes

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.

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 organization 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 key management protocols, security of the management plane and assessment models and techniques,
  - 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 standardization activities by many different organizations 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 organization 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-organization (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.

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

3.2.2. Design and evaluation of P2P-based management architectures

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 decentralized 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 centralized 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.

3.2.3. 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.

3.2.4. 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 makes 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 optimize 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 management

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. Extension 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.

Since 2006 we have also started an activity on security assesment. The objective is to investigate new methods and models for validating the security of large scale dynamic networks and services. The first targeted service is VoIP.

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 at 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 synchronization. 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,
4. voice over IP infrastructure.

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.

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. JDukeBox

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

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 Inria's libresource forge (http://libresource.inria.fr).

5.2. NetSV

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

NetSV is a distributed monitoring framework for IPv6 network renumbering supervision. The development was initiated during the 6Net IST Project, and was pursued in 2006 thanks to Cisco Systems sponsorship.

Our framework is able to follow the renumbering procedure step by step as defined in RFC 4192. It helps administrators to validate each one of these steps. *NetSV* is composed of three entities: a manager, a set of distributed agents and some diagnostic tools. The manager, written in Python, collects the information and alarms sent by the agents and displays them on a dynamic WEB interface. This graphical interface allows the administrator to pilot the agents and the diagnostic tools. Distributed agents are running on all hosts of a network. They continuously monitor the local addressing and the messages sent by the routers, and send reports to the manager. The diagnostic tool acts as a standalone tool or as a module of the agent. It is also in charge of dynamically verifying the running services and their configuration on a host if a renumbering is performed. The agent and the diagnostic tool have been written in C. XML is used by the framework for the configuration files and for all data exchange between the components.

The software package and its source code is freely distributed under an opensource license (LGPL) at http://netsv.sourceforge.net/.

5.3. NDPMon

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

The Neighbor Discovery Protocol Monitor (NDPMon) is an IPv6 implemention of the well-known ArpWatch tool. NDPMon monitors the pairing between IPv6 and Ethernet addresses (NDP activities: new station, changed Ethernet address, flip flop...). NDPMon also detects attacks on the NDP protocol, as defined in RFC 3756 (bogon, fake Router Advertisements...). An XML file describes the default behavior of the network, with the authorized routers and prefixes, and a second XML document containing the neighbors database is used. This second file can be filled during a learning phase. All NDP activities are logged in the syslog utility, and so the attacks, but these ones are also reported by mail to the administrator. Finally, NDPMon can detect stack vulnerabilities, like the assignment of an Ethernet broadcast address on an interface.

The software package and its source code is freely distributed under an opensource license (LGPL). It is implemented in C, and is available through a SourceForge project at http://ndpmon.sf.net. An opensource community begins to spring, and we are working on the integration of the software in GNU/Linux distributions. We will pursue the implementation of this tool, maintain it, and bring new features and improvements to it.

5.4. rmidump

Participants: Laurent Andrey [contact], Mathieu Colonna, Abdelkader Lahmadi.

The rmidump utility is two folded:

1. A Java library which reads network trace files (pcap format) and extracts Java Remote Method Protocol (JRMP) data and allows easy trace of Java Remote Invocations (RMI). This library can be used to write **network level** analysers of RMI calls latency for a given application for example.
2. a Wireshark[2] (former ethereal) plugin which pins-out packets related to RMI/JRMP and deserializes return values or parameters as best as possible.

A first draft release of this utility wiil soon be available as a tarball of source code on the Madynes web site http://madynes.loria.fr. The Java lib is obviously portable on any platform where Java is available. The Wireshark plugin is written in C and strictly follows the Wireshark coding rules and should be compilable on any platform Wireshark has been ported.

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 focused on providing a uniform security continuum independent of the underlying management protocol and interface.

In 2006, we worked on two main issues, namely formal approaches to define, assure and evaluate security policies for the management plane. First, a generic RBAC model was defined and thus mapped to individual security for different management frameworks. We defined a formal model and individual mappings for SNMP, NetConf and some proprietary vendor specific interfaces. We evaluated the performance of security features in Netconf and built a full fledged open source NetConf implementation. The main publications related to this activity are [18], [16], [17], [47].

[2] http://www.wireshark.org

We have also performed a large scale analysis of both backscatter traffic and a distributed honeypot. We analysed large datasets with packet capture traces in order to detect patterns of network configurations at an Internet level scale. Such patterns are related to misconfigured firewalls, routers, NAT devices and Internet facing servers. The results of this activity are published in [35], [56].

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. Several new sensitive applications require group communications and are deployed in ad hoc networks: wireless networks formed spontaneously, without any fixed infrastructure, and which can be highly mobile. A high level of security is often required in such applications, like military or public security applications. The most suitable solution to ensure these protected services is the deployment of a group key management protocol, adapted to the characteristics of MANETs, and especially to the mobility of nodes.

In our previous work, we defined OMCT (Optimized Multicast Cluster Tree), an algorithm for dynamic clustering of multicast group, that takes into account the nodes localization and mobility, and optimizes the energy and bandwidth consumptions. We also specified a group key management protocol BALADE, dedicated to operate in ad hoc networks, to secure multicast communications, according to the sequential multi-source model.

Then, we integrated OMCT (Optimized Multicast Cluster Tree) within our group key management protocol BALADE. This integration of BALADE and OMCT allows an efficient and fast key distribution process, which was validated through simulations by applying various models of mobility (individual mobility and group mobility). These results showed a high dependence between the mobility model and the behavior of the key distribution protocol [13].

We showed how our scheme could be combined with the Multipoint Relaying technique, in a very effective way, according to the localization of the group members and their mobility. The efficiency of this combination in terms of average latency of key delivery, energy consumption and key delivery ratio, was validated through simulation [27].

Emerging applications require secure group communications involving hierarchical architecture protocols. Designing such secure hierarchical protocols is not straightforward, and their verification becomes a primordial issue in order to avoid any possible security attack and vulnerability. Several attempts have been made to deal with formal verification of group protocols, but, to our knowledge, none of them did concern hierarchical ones. Therefore, we addressed the specific challenges and security issues of the protocols used within hierarchical secure group communications and of their verification and validation. We chose the back-end AtSe of the AVISPA tool, to verify one of these protocols, as it enables to deal with the exponentiation of Diffie-Hellman often used in group key management[26]. This work was done in the context of the SAFECAST project and is the result of collaboration between the CASSIS and MADYNES teams. We also evaluated the performances of the hierarchical group key management protocol defined in the SAFECAST project with the network simulator NS2 [42].

6.3. Management benchmarking and performance models

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

In 2006, the activity around management benchmarking focused on:

1. extension of our test methodoly and test suite for a scale related test factor: the number of managed nodes.
2. most relevant metrics for our domain.

The first achievement lead us to adapt our existing JMX test suite on a computer grip facility (french grid5000). This work has been published in [33], [20]. A tool to allow us to do network level measurement for Java Remote Invocation (RMI) request (JMX is using RMI) has been developed in this context.

The second achievement in management performances analysis is an indepth investigation of delays introduced by management platforms. These delays are of importance in monitoring applications, since they impact the quality of what such applications can observe. We also tried to model delays as a random variable in order to provide input for future simulation.

These two achievements will enable us to adapt the scalabily metrics proposed in [60] based on a $Production \times Quality/Cost$ scheme to compare various management framework profiles.

6.4. Management of peer-to-peer overlays

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

The PhD defence of Guillaume DOYEN [11] on management of peer to peer (P2P) network and services took place in december 2005. Results of this work was exploited during the year 2006 toward an implementation work. Our generic information model for the P2P has been extended to specify the existing Jxta P2P framework [31]. Generic concepts as peer, community or services had to be seamlessly adapted into Jxta concepts. However other concepts, especially Jxta communication pipes was not as generic as our model and we had to add more semantic in order to match with the Jxta reality. Our implementation provides all Java object classes that model Jxta framework, part of this work is done in an automatic way from our language independant specifications (with the Common Information Model). Such produced classes only exhibit interfaces and we had to complete with intrumentation procedures in order to find out necessary information inside Jxta framework.

At the organizational point, we designed a new management paradigm where there is no more statically designed managers managing several agents but only one dynamically elected manager from all peers present in a Jxta community (we plan to extend this by the election of several dynamic managers). Each time a new peer joins a community, it asks for a manager and if one is already present it responds to the new peer. If no response is received then the new peer announces to the community that it is now the manager. Each manageable peer should so provide its set of management interfaces to the manager and this latter should infer shared object between several peers, as a Jxta communication pipes. We plan to share our implementation with the Jxta community.

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 defining a new management concept relying on probabilistic mechanisms, which we call probabilistic management. The key idea is to elaborate a new management approach, where only a subset of the nodes are under the control of a manager. These nodes are determined based on temporal and spatial criterium, such that the manager has a logical connectivity with the managed nodes. We have analysed several manager election algorithms with respect to mobility models, parameters (speed, pause time, spatial dimensions) and standard simulation scenarios. The obtained results give probabilistic guarantees about the percentage of nodes that can be managed within the first two main components. These results were published in [23], [12]. Paper [23] received the best student paper award at the IFIP/IEEE NOMS'06 symposium.

The second research activity addressed the fault management in ad-hoc networks. Fault management in ad-hoc network is much more challenging since ressource limitations and out of coverage conditions have to be considered and addressed. An out of coverage node is unreachable, but this is not due to a fault or an outage. The main issue that has to be addressed is to differentiate normal from abnormal behavior in an additonal presence of malicious/non-cooperative nodes. A managed node might not provide the requested management information either because of limited technical capabilities or because of intended malicious purpose. Our

approach defined an information theoretical framework leveraging the Shannon entropy coupled with a self-organizing management management capable to deal with rogue/false information. The relevant publication is [22].

6.6. Autonomous management

Participants: Laurent Ciarletta [contact], Olivier Festor.

In 2006, we have achieved several milestones regarding our work on the self-organization of the management plane in the scope of the Swan project. This final work has been focused on autonomic inter-domain configuration and monitoring of QoS-oriented services (video-conference). It has lead to the definitions of a Web Service-based architecture and an algorithm based on dynamic programming to negotiate configuration and monitoring parameters [30], [29].

Although initial security issues have been set aside in favor of QoS matters in the final year of SWAN, a more global state of the art regarding security in autonomic computing has been published in a scientific book [15].

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 still pursuing our investigations on this domain and have been working more specifically on three prospects:

- securing the access to the pervasive computing world with a simple secure infrastructure for the pervasive virtual office [14],
- co-simulations of these pervasive computing environments (including the users in the simulations). We have focused on the collaborative simulations of dynamic networks/elements, namely P2P or adhoc networks using agents to drive those simulations [58],
- state of the art and first experiments around geolocalization with WiFi that will be integrated with Service Discovery protocols [57].

6.8. Voice over IP Security

Participants: Humberto Abdelnur, Mohamed Nassar, Olivier Festor, Radu State [contact].

VoIP inherits the adjacent security problems associated with the IP as well as new VoIP specific ones. Attackers can profit from the vulnerabilities of the VoIP protocols and architectures. Both signaling protocols such as SIP (Session Initiation Protocol) and H.323 and media transport protocols such as RTP and RTCP could be the target of a wide set of attacks, ranging from eavesdropping, denial of service, fraudulent usage and SPIT (Spam over internet telephony). Important work in both host and network intrusion detection has been already done by the industrial and academic research community, focused in scope towards network intrusion detection for transport, routing and application level protocols. Security assessment techniques and approaches have been already deployed in the operational landscape and had been the subject of the research community. However, specific approaches for VoIP are still an incipient stage and we were motivated in our to work to leverage existing conceptual solutions for the VoIP specific application domain.

Our research work addressed two main directions. The first is concerned with automated security assessment and penetration testing for VoIP. We have developed a conceptual approach and a fully operational prototype. These results were published in [19], [37].

A second direction of research consisted in the development of conceptual models for VoIP intrusion detection. We proposed a bayesian based intrusion detection system and ongoing work is done towards a VoIP specific honeypot. Preliminary research results were published in [34].

6.9. Worm based network management

Participants: Olivier Festor, Radu State [contact].

While worms and their propagation have been a major security threat over the past years, causing major financial losses and down times for many enterprises connected to the Internet, we consider that valuable lessons can be learned from them and that network management, which is the activity supposed to prevent them, can actually benefit from their use. We analysed how it has been addressed in standard management frameworks, we identified their limits and describe how current malware already provides efficient solutions to these limits. We instantiate a case study on a realistic application of worm based network management. The current publication on this issue is [36].

7. Contracts and Grants with Industry

7.1. SAFARI

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

Dates February 2003 - 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 2006, we did continue to investigate distributed management approaches for ad-hoc network, especially for faulty node identification (see related section in “New results”). We also completed all the implementations for this project, namely a full JMX instrumentation of the JXTA P2P infrastructure and a key distribution protocol for multicast services. The later was implemented on top of a collaborative distributed Jukebox developped in our team: JDukebox. The experience gained on developing this tool has been published in [25].

All documents, software components and contributions to deliverables were provided on time. The project has completed on April 30th, 2006.

7.2. 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 2006, we contributed to the writing of a document related to the different modeling techniques and simulation/validation tools applicable to the security [41].

In collaboration with the LAAS laboratory, we validated the SAFECAST functional architecture through two tools: AVISPA and TURTLE and we studied the complementarity of both tools [44]. AVISPA takes into account security aspects and TURTLE the time constraints.

7.3. MUSE

Participants: Humberto Abdelnur, Vincent Cridlig, Olivier Festor [contact].

Dates January 2006 - December 2007

Partners Alcatel (leader), 10 universities, 5 system vendors, 2 component vendors, 9 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 standardization.

The MADYNES group is contributing to this second phase of the project project on:

- the design of a multi-provider model access control model for home gateway configuration,
- the design of an interoperability model enabling home gateways managed through the ATM-Forum TR-69 to be accessible over the IETF emerging Netconf standard configuration protocol.

For the multi-provider access model we did propose the use of an RBAC model and did specify all the necessary standard extensions needed in TR-69 to support the proposed model. Within the project, a subset of the proposed RBAC model was selected by the partners for integration in the platform. Its implementation will be done by one participating equipment provider.

To enable TR69-based devices to be managed through Netconf, we have specified a full gateway together with dedicated new Netconf capabilities.

All specifications were completed in 2006 and are documented in the DB3.4 deliverable [54] of the project which was edited by Olivier Festor and Sam D'Haseleer. Implementation of the TR-69/Netconf gateway will start in early January 2007. The madynes' Ensuite platform will be used for the Netconf side of the implementation.

7.4. AIRNET

Participants: Olivier Festor [contact], Christian Popi.

Dates June 2006 - May 2009

Partners LSR-IMAG (Leader), LIP6, UniversitÂ Pierre et Marie Curie, EurÂcom, LSIIT, INRIA (MADYNES), Division R&D de France TÂlÂcom, Thales Communications, Ozone

Airnet is a french collaborative research project funded by the RNRT-ANR. The objective of this project is to study the design, deployment and operation of a full wireless interconnection infrastructure over a public frequency.

The MADYNES contributions to this project are:

- the design of a distributed self-configuration model and its implementation based on the Netconf model;
- the investigation of distributed monitoring for fault management and mesh-networks security assessment.

This work is part of the configuration management and security management themes of the MADYNES group. In 2006, we have extended our Netconf suite to enable its use in a cooperative way. Christian Popi started to work on the management aspects of mesh networks in October 2006.

7.5. SWAN: Self aWare mAnagemeNt

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

Dates January 2004 - October 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 three 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 deployment.

We contributed to:

- the definition of a self-organizing management plane for cross-domain services: algorithm and architecture
- 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.

7.6. CISCO

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

Dates January 2006 - December 2006

Partners CISCO Systems

Starting on the 1st of January 2006, with Cisco sponsorship, we continued the study on IPv6 renumbering we began during the 6NET IST project in 2005, while focusing on the network's security architecture. Our goal was to design and implement a self configurable management architecture to enable an automatic monitoring and management of an IPv6 network renumbering procedure.

We concentrated our efforts on two parts: Security and Monitoring.

Concerning Security, we focused on firewalls and their update during a renumbering procedure. This study has led to the definition of firewall access rule rewriting guidelines, in order to modify the routers' Access-Lists according to the ongoing renumbering, or raise alarms if needed. Based on these guidelines, we implemented an update engine while designing a generic data model for Firewall Rules. We used Netconf to apply the modifications on the devices. To do so, we extended the manager part of the Madynes EnSuite Netconf framework to integrate this engine and to interact with the Cisco Enhanced Device Interface, a Netconf Proxy developed by Cisco.

During the study on monitoring, we pursued the development of NetSV, a distributed monitoring framework for IPv6 renumbering. In order to test the new firewall rules generated with the generic update engine, we developed some traffic probes, which we are planning to integrate as a module in NetSV. Our main task on this topic was the implementation of NDPMon, the Neighbor Discovery Protocol Monitor. This tool is an IPv6 version of the well-known ArpWatch, and monitors the pairing between IPv6 and Ethernet addresses and detects attacks on the NDP protocol.

The results obtained during this study has been successfully demonstrated during October 2006 to our CISCO partners, and a follow-up to this investigation is about to be agreed. They have been published in the following conference paper and technical reports: [24], [38], [38], [40].

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

8. Other Grants and Activities

8.1. EMANICS

Olivier Festor is the initiator and the scientific leader of the EMANICS Network of Excellence. EMANICS 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.

EMANICS is now running for one year and has reached many great successes in the area of researchers and community integration, joint research results, outstanding publications quality and score, standard contributions, operational testbeds, visibility and recognition. Details on the networks and its achievements can be found on the networks Web site at : http://www.emanics.org.

8.2. International relationships and cooperations

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

We actively participate to the Internet Research Task Force (IRTF) Network Management Research Group (NMRG). We participated in two events of the NMRG this year. One was the meeting at the 66th IETF in Montreal dedicated to SNMP trace collection and analysis. The second meeting we attended was a joint EMANICS/NMRG workshop on the Research challenges for network and service management. This workshop was help in Utrecht in October 2006.

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. Isabelle Chrismen is member of EUNICE technical committee.

MADYNES is also 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. In 2006, we did participate to the joint CNRS-INRIA-WIDE workshop (18 & 19 September 2006, Paris, France) and present our results in Ad-Hoc networks management and our developments in Netconf-based software solutions.

8.3. National initiatives

In addition to the cooperation with the various partners within national ANR-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 (RESCOM) CNRS-INRIA summer school which was held in June 2006 in Porquerolles. The team is regularly contributing to the organization of the school and is a contributor to several tutorials given during the school week. Laurent Andrey, Isabelle Chrisment, Vincent Cridlig, Olivier Festor and Radu State did participate to this year's event. Radu State gave a tutorial entitled: Viral Epidemiology.

Olivier Festor is member of the board of the INRIA-Alcatel cooperation as part of the Alcatel research partnership. He also member of the ANR-RNRT commission 4 on *software for telecommunications*.

Isabelle Chrisment was a reviewer for the ANR-RNRT 2006 selection process.

8.4. Guest Researchers

Aiko Pras, senior researcher at the University of Twente, The Netherlands spent 4,5 months on sabattical in the team (July to November 2006). This sabattical was partially funded by the EMANICS network of excellence. During his stay, Aiko Pras worked essentially with Laurent Andrey and Abdelkader Lahmadi on management frameworks benchmarking. The outcome of this joint research is a common definition of management benchmarking metrics which were defined by MADYNES members and their application to SNMP-based management which is Aiko Pras' area of expertise. A technical report and a joint publication on this common work are under preparation.

Tiago Fioreze, Ph.D. Student from The University of Twente spent one week in the team (in October 2006) to share with MADYNES members the self-management aspects of his thesis. This stay was also funded by the EMANICS network of excellence.

Jérôme François spent three month at the dePaul University in Chicago and Waterloo, working on distributed firewall configuration.

9. Dissemination

9.1. Program committees and conference organization

Radu State was in the organizating committee for NOMS 2006 where he was publication co-chair together with Oliver Festor.

Radu State was the TPC co-chair for two events in 2006. He co-chaired the 17 th IEEE/IFIP DSOM 2006 workshop, which is the flagship workshop of the network management comunity. He did co-chair the 1 st IEEE workhop on VoIP security and management, VoIP MaSE 2006. He was technical program comittee of the following confernces: IFIP/IEEE NOMS 2006, IEEE APNOMS 2006, ICNS 2006, IntellComm2006, IEEE/IFIP E2EMon 2006, NOMS 2006 Application.

Isabelle Chrisment was member of the program committee of the following events: SAR 2006, NOTERE 2006 and VoIPMaSe 2006. She is also member of the scientific board of SAR.

In 2006, Olivier Festor was member of the following program committees: IFIP/IEEE IM'2006, IFIP/IEEE NOMS 2006, CFIP'2006, NOTERE 2006, GRES 2006, DNAC'2006, E2EMo2006, VoIPMase2006. At DSOM'2006, he chaired a session on "Supporting approaches for network management". He was also member of the following new conferences SIGCOMM 2006 - Workshop on Internet Network Management (INM'06), IEEE / IST Workshop on Monitoring, Attack Detection and Mitigation (MONAM), First International Workshop on Feedback Control Implementation and Design in Computing Systems and Networks (co-located with NOMS'06), International Conference on Networking and Services (ICNS 2006), Advanced International Conference on Telecommunications (AICT 2006).

Olivier Festor is also member of the Board of Editors of the Journal of Systems and Network Management and reviewed 35 papers for several international conferences and journals in 2005.

Laurent Andrey was member of the TPC of *Atelier OSGI*, CNAM, Paris, September 5, 2006.

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 (master research). 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[3] 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.

André Schaff is the Director of the ESIAL Engineering School.

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.

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

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:

- In 2006, Radu State gave a tutorial on Internet Worms at the RESCOM summer school.
- Olivier Festor was a panelist at the DSOM'2006 Panel entitled "Research challenges in network management".
- Frédéric Beck, Julien Delove and Isabelle Chrisment presented the JDukebox on a mobile IPv6 infrastructure at JRES in December 2005 [28].
- In 2006, Radu State gave within the Emanics NoE classes in University of Pitesti on topics related to: VOIP, Internet worms, intrusion detection.
- In 2006, Isabelle Chrisment gave a talk about how to monitor IPv6 renumbering at French IPv6 Summit, Cannes.

9.4. Commissions

The following Ph.D Degree defenses were held by members of the team:

- Rémi BADONNEL, Ph.D. in Computer Science from the Henri Poincaré University Nancy 1. Title: *Supervision des Réseaux et Services Ad-Hoc*, Committee: Karl Tombre (president), Serge Fdida (reviewer), Philippe Jacquet (reviewer) André Schaff, Radu State, December 2006.
- Mohamed Salah BOUASSIDA, Ph.D. in Computer Science from the Henri Poincaré University Nancy 1. Title: *Sécurité des communications de groupe dans les réseaux ad hoc*, Committee: René Schott (president), Abdelmadjib Bouabdallah (reveiwer), Maryline Maknavicius-Laurent (reviewer), Isabelle Chrisment, Olivier Festor, Pierre de Saqui-Sannes, December 2006.
- Vincent CRIDLIG, Ph.D. in Computer Science from the Henri Poincaré University Nancy 1. Title: *Sécurité du plan de gestion des réseaux IP*, Committee: Claude Godart (president), Omar Cherkaoui (reviewer), Frédéric Cuppens (reviewer), Olivier Festor, Stéphane Frénot, Radu State, December 2006.
- Guillaume DOYEN, Ph.D. in Computer Science from the Henri Poincaré University Nancy 1. Title: *Supervision des réseaux et services pair à pair*, Committee: Nacer Boudjlida (president), Michèlle Sibilla (reviewer), François Spies (reviewer), Olivier Festor, Stéphane Frénot, Emmanuel Nataf, December 2005.

Team members participated to the following Ph.D. commissions:

- Emmanuel LAVINAL, Ph.D. in Computer Science from Université Paul Sabatier - Toulouse III. title: *Un cadre organisationnel générique multi-agents pour une gestion autonome de réseaux et de services* , Committee: F. Krief (reviewer), J. Ferber (reviewer), Olivier Festor (committe president and reviewer), M. Salaun , T. Desprats , Y. Raynaud, July 2006.
- Hahnsang KIM, Ph.D. in Computer Science from Université d'Evry-Val d'Essonne. Title: *An authentication architecture for cross-domain mobility*, Committee: Refik Molva (reviewer), I. Chrisment (reviewer), Kaisa Nyberg, P. Urien, J. Araujo, K. G. Shin, H. Afifi, April 2006.
- Zainab KHALLOUF, Ph.D. in Computer Science from Institut National Polytechnique de Grenoble. Title: *Secure multicast routing infrastructure: the network operator point of view*, Committee: G. Mazaré, I. Chrisment (reviewer), B. Cousin (reviewer), O. Paul, A. Duda, V. Roca, S. Loye, March 2006.
- Julien LAGANIER, Ph.D. in Computer Science from Ecole Normale Supérieure de Lyon. Title: *Architecture de sécurité décentralisée basée sur l'identification cryptographique*, Committee: C. Casteluccia, S. Fdida, O. Festor (reviewer), M. Maknavicius-Laurent (reviewer), P. Vicat-Blanc Primet, March 2006.

- Zakaria BENAHMED DAHO, Ph.D. in Computer Science from Ecole Nationale Supérieure des Télécommunications. Title: *Vers une nouvelle génération de service pour une auto-gestion de bout-en-bout*, Committee: O. Festor (reviewer), G. Pugolle (reviewer), M. Sibilla (reviewer), N. Simoni, January 2006.

Team members reviewed the following Ph.D. thesis:

- Udaya TUPAKULA, Ph.D. in Computer Science from Macquarie University. Title: *Modeling, design and implementation techniques for counteracting denial of service attacks in network*.
- Georgios RODOLAKIS, Ph.D. in Computer Science from Ecole Polytechnique. Title: *Analytical Models and Performance Evaluation in Massive Mobile Ad Hoc Networks*, Committee: Anthony Ephremides (reviewer), Olivier Festor (reviewer), Wojciech Szpankowski (reviewer), Philippe Jacquet, Kaldoun Al Agha, Laurent Viennot, December 2006.

MADYNES members were members of the following Habilitation Degree commission:

- Philippe OWESARSKI, Habilitation Degree in Computer Science from Université Paul Sabatier - Toulouse III. Title: *Contribution de la métrologie Internet á l'ingénierie des réseaux*, Commission d'examen : A. Benzekri (président), M. Diaz , S. Fdida (reviewer), O. Festor (reviewer), G. Leduc, F. Lepage (reviewer), September 2006.
- Ahmed MEHAOUA, Habilitation Degree in Computer Science from Université de Versailles á Saint Quentin. Title: *Transport et contrôle de la qualité des services vidéo sur les réseaux ATM, IP et WLAN*, Committee : R. Castanet (reviewer), K. Chen (reviewer), O. Festor (reviewer), D. Seret , R. Boutaba , J-P. Claude , G. Pujolle, S. Thome, December 2005.

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, N. ROUSKAS (editors). , Lecture Notes in Computer Science, vol. 3042, Springer-Verlag, May 2004, p. 725-742.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

Year Publications

Books and Monographs

[7] R. STATE, S. VAN DER MEER, D. O'SULLIVAN, T. PFEIFFER. *Large Scale Management of Distributed Systems*, Lecture Notes in Computer Science, vol. 4269, Springer, 2006, http://hal.inria.fr/inria-00107015/en/.

Doctoral dissertations and Habilitation theses

[8] R. BADONNEL. *Supervision des Réseaux et Services Ad-Hoc*, Ph. D. Thesis, Université Henri Poincaré - Nancy I, december 2006.

[9] S. BOUASSIDE. *Sécurité des communications de groupe dans les réseaux ad hoc*, Ph. D. Thesis, Université Henri Poincaré - Nancy I, december 2006.

[10] V. CRIDLIG. *Sécurité du plan de gestion des réseaux IP*, Ph. D. Thesis, Université Henri Poincaré - Nancy I, december 2006.

[11] G. DOYEN. *Supervision des réseaux et services pair à pair*, Ph. D. Thesis, Université Henri Poincaré - Nancy I, december 2005.

Articles in refereed journals and book chapters

[12] R. BADONNEL, R. STATE, O. FESTOR. *Self-Organized Monitoring in Ad-Hoc Networks, Modeling, Analysis, Design and Management*, in "Telecommunication Systems", vol. 30, n^{o} 1-3, november 2005, p. 143-160, http://hal.inria.fr/inria-00090223/en/.

[13] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *Mobility-Awareness in Group Key Management Protocols within MANETs*, in "Annals of Telecommunications", vol. 61, n^{o} 9-10, 2006, p. 1151-1173, http://hal.inria.fr/inria-00105923/en/.

[14] L. CIARLETTA, A. BENSLIMANE. *Management, Control and Evolution of IP Networks*, G. PUJOLLE (editor). , chap. A secure infrastructure for the pervasive virtual office, ISTE, 2006, http://hal.inria.fr/inria-00106782/en/.

[15] L. CIARLETTA. *L'autonomie dans les réseaux*, F. KRIEF, M. SALAÜN (editors). , I2C (Information, Commande, Communication), chap. Sécurité et Autonomic Computing, Hermes Science, 2006, p. 107-131, http://hal.inria.fr/inria-00112173/en/.

[16] V. CRIDLIG, H. ABDELNUR, R. STATE, O. FESTOR. *XBGP-MAN: A XML management architecture for BGP*, in "International Journal of Network Management", vol. 16, n^{o} 3, 2006, http://hal.inria.fr/inria-00001223/en/.

[17] V. CRIDLIG, R. STATE, O. FESTOR. *Ensuite, une plateforme libre de configuration de réseau*, in "Techniques de l'ingénieur", 2006, http://hal.inria.fr/inria-00090142/en/.

[18] V. CRIDLIG, R. STATE, O. FESTOR. *Role-Based Access Control for XML Enabled Multi-Protocol Management Gateways, Adapting to Dynamic Environments*, in "IEEE eTransactions on Network and Service Management", vol. 3, n^{o} 1, 2006, http://hal.inria.fr/inria-00001222/en/.

Publications in Conferences and Workshops

[19] H. ABDELNUR, V. CRIDLIG, R. STATE, O. FESTOR. *VoIP Security Assessment: Methods and Tools*, in "The 1st IEEE workshop on VoIP Management and Security: VoIP MaSe, 2006, Vancouver/Canada", S. NICCOLINI, H. SCHULZRINNE, R. STATE (editors). , Published on CDROM only, IEEE Communications Society, IEEE/IFIP, 2006, http://hal.inria.fr/inria-00001224/en/.

[20] L. ANDREY, O. FESTOR, A. LAHMADI. *Evaluation du passage à l'échelle des systèmes de gestion : métriques et modèles*, in "Colloque Francophone sur l'Ingénierie des Protocoles - CFIP 2006, 2006-10-29, Tozeur/Tunisia", Hermes, Eric Fleury and Farouk Kamoun, 2006, http://hal.inria.fr/inria-00105550/en/.

[21] L. ANDREY, A. LAHMADI, O. FESTOR. *On Delays in Management Frameworks: Metrics, Models and Analysis*, in "17th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management - DSOM 2006, 2006-10-22, Dublin/Ireland", Springer, 2006, http://hal.inria.fr/inria-00105535/en/.

[22] R. BADONNEL, R. STATE, O. FESTOR. *Fault Monitoring in Ad-Hoc Networks based on Information Theory*, in "5th International IFIP-TC6 Networking Conference (Networking'06), 2006-05-15, Coimbra/Portugal", F. BOAVIDA, T. PLAGEMANN, B. STILLER, C. WESTPHAL, E. MONTEIRO (editors). , in: Lecture Notes in Computer Science, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems, vol. 3976, Springer, Edmundo Monteiro, 2006, p. 427-438, http://hal.inria.fr/inria-00090211/en/.

[23] R. BADONNEL, R. STATE, O. FESTOR. *Probabilistic Management of Ad-Hoc Networks*, in "10th IEEE/IFIP Network Operations and Management Symposium - NOMS 2006, 2006-04-03, Vancouver/Canada", J. HELLERSTEIN, B. STILLER (editors). , Management of Integrated End-to-End Communications and Services, Best Student Paper Award, IEEE, Raouf Boutaba, 2006, http://hal.inria.fr/inria-00090206/en/.

[24] F. BECK, I. CHRISMENT, O. FESTOR. *A Monitoring Approach for Safe IPv6 Renumbering*, in "IPv6 Today - Technology and Deployment, 2006-08-01, Bucharest/Romania", 2006, http://hal.inria.fr/inria-00106170/en/.

[25] F. BECK, V. DELOVE, I. CHRISMENT, O. FESTOR. *Couplage Multicast et Mobilité IPv6 dans la plate-forme pair-à-pair JDukeBox*, in "6ème Conférence Internationale sur les NOuvelles TEchnologies de la REpartition - NOTERE'2006, 2006-06-07, Toulouse/France", 2006, http://hal.inria.fr/inria-00113204/en/.

[26] M. S. BOUASSIDA, N. CHRIDI, I. CHRISMENT, O. FESTOR, L. VIGNERON. *Automatic Verification of Key Management Architecture for Hierarchical Group Protocols*, in "Sécurité et Architecture des Réseaux - SAR 2006, 2006-05-06, Seignosse/France", 2006, p. 381-397, http://hal.inria.fr/inria-00090165/en/.

[27] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *Efficient Group Key Management Protocol in MANETs using the Multipoint Relaying Technique*, in "5th International Conference on Networking - ICN 2006, 2006-04-23, Ile maurice", I. C. SOCIETY (editor). , 2006, 64, http://hal.inria.fr/inria-00090141/en/.

[28] I. CHRISMENT, F. BECK, J. DELOVE. *Mobilité et Multicast Ipv6*, in "JRES 2005", 2005, http://hal.inria.fr/inria-00113641/en/.

[29] L. CIARLETTA, S. PIEKAREC, A. AGHASARYAN, H. POUYLLAU, S. HAAR, E. FABRE, N. MBAREK. *Multi-Domain Self Aware Management : Negotiation and Monitoring*, in "13th International Conference on Telecommunications - ICT 2006, 2006-05-16, Funchal, Madeira island/Portugal", 2006, http://hal.inria.fr/inria-00106791/en/.

[30] L. CIARLETTA, H. POUYLLAU, A. AGHASARYAN, S. HAAR. *X-domain QoS budget negotiation using Dynamic Programming*, in "Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services - AICT 2006 / ICIW 2006, 2006-02-19, Guadeloupe/French Caribbean", IEEE Computer Society, 2006, 35, http://hal.inria.fr/inria-00106789/en/.

[31] G. DOYEN, E. NATAF, O. FESTOR. *Supervision des réseaux et services pair à pair : application à la plate-forme JXTA*, in "Colloque Francophone sur l'Ingénierie des Protocoles - CFIP 2006, 2006-10-30, Tozeur/Tunisia", Session 10 : gestion & supervision, Hermès, Eric Fleury and Farouk Kamoun, 2006, 12 p, http://hal.inria.fr/inria-00113390/en/.

[32] G. DOYEN, E. NATAF, O. FESTOR. *Supervision des réseaux et services pair à pair : application à la plate-forme Jxta*, in "Colloque Francophone sur l'Ingénierie des Protocoles - CFIP 2006, 2006-10-30, Tozeur/Tunisie", 2006, http://hal.inria.fr/inria-00102649/en/.

[33] A. LAHMADI, L. ANDREY, O. FESTOR. *Une approche de benchmarking des pratiques de gestion basées sur un middleware JMX pour les services et les applications*, in "Nouvelles Technologies de la Répartion - NOTERE 2006, 2006-06-06, Toulouse/France", L. APVRILLE, K. DRIRA, P. DE SAQUI-SANNES, T. VILLEMUR (editors). , Nouvelles Technologies de la Répartition, n^{o} 6, LAAS-CNRS et l'ENSICA, 2006, p. 145-151, http://hal.inria.fr/inria-00090144/en/.

[34] M. E. B. NASSAR, R. STATE, O. FESTOR. *Intrusion detection mechanisms for VoIP applications*, in "Third annual VoIP security workshop - VSW'06, 2006-06-01, Berlin/Allemagne", Fraunhofer FOKUS, 2006, http://hal.inria.fr/inria-00107054/en/.

[35] R. STATE, J. FRANCOIS, O. FESTOR. *Tracking global wide configuration errors*, in "IEEE / IST Workshop on Monitoring, Attack Detection and Mitigation, 2006-09-28, Tubingen/Germany", 2006, http://hal.inria.fr/inria-00107005/en/.

[36] R. STATE. *Lessons from malware*, in "1st International Workshop on the Theory of Computer Viruses, 2006-05-04, Nancy/France", Yes, 2006, http://hal.inria.fr/inria-00110954/en/.

[37] R. STATE. *VoIP Security Assessment and Intrusion Detection*, in "Journée Sécurité des Systèmes d'Information - JSSI 2006, 2006-11-28, Bruz/France", 2006, http://hal.inria.fr/inria-00110958/en/.

Internal Reports

[38] F. BECK, I. CHRISMENT, O. FESTOR. *IPv6 Renumbering - Security and Monitoring. D1.1 - Scenarios and avoidance procedures*, Contract Report, 2006, http://hal.inria.fr/inria-00113215/en/.

[39] F. BECK, I. CHRISMENT, O. FESTOR. *IPv6 Renumbering - Security and Monitoring. D1.2 - Functional Architecture*, Contract Report, 2006, http://hal.inria.fr/inria-00113221/en/.

[40] F. BECK, I. CHRISMENT, O. FESTOR. *IPv6 Renumbering - Security and Monitoring. D2.1 - Rules rewriting. D2.2 NetConf integration*, CISCO, Research Report, 2006, http://hal.inria.fr/inria-00113225/en/.

[41] A. BOUABDALLAH, M. S. BOUASSIDA, I. CHRISMENT, P. DE SAQUI-SANNES, S. MOTA, H. RAGAB HASSAN, A. SERHROUCHNI, T. VILLEMUR. *L4.3 : Identification et mise en oeuvre des outils de simulation et vérification*, Projet RNRT SAFECAST, Contract Report, 2006, http://hal.inria.fr/inria-00113243/en/.

[42] M. BOUALI. *Evaluation d'un protocole hiérarchique de distribution de clé de groupe dans les MANETs*, projet RNRT SAFECAST, Internship Report, 2006, http://hal.inria.fr/inria-00113208/en/.

[43] S. M. BOUASSIDA, I. CHRISMENT, O. FESTOR. *Validation de BALADE Protocole de gestion de clés de groupe dans les réseaux ad hoc*, Rapport de recherche INRIA, n^{o} RR-5896, 2006, http://hal.inria.fr/inria-00071372/en/.

[44] M. S. BOUASSIDA, B. FONTAN, I. CHRISMENT, P. DE SAQUI-SANNES, S. MOTA, T. VILLEMUR. *L4.1 : Validation fonctionnelle de l'architecture*, Projet RNRT SAFECAST, Contract Report, 2006, http://hal.inria.fr/inria-00113244/en/.

[45] T. CHOLEZ. *Développement de l'outil NdMon du projet MADYNES*, Internship Report, 2006, http://hal.inria.fr/inria-00113091/en/.

[46] M. COLONNA. *RMI Dump*, Internship Report, 2006, http://hal.inria.fr/inria-00105918/en/.

[47] V. CRIDLIG, H. ABDELNUR, R. STATE, O. FESTOR. *Assessment of security extended XML-based Management*, Research Report, 2006, http://hal.inria.fr/inria-00084004/en/.

[48] N. DAGORN. *Analyse commentée de l'article : "Adaptive, Model-based Monitoring for Cyber Attack Detection"*, Research Report, 2006, http://hal.inria.fr/inria-00084204/en/.

[49] N. DAGORN. *Détection et prévention d'intrusion : présentation et limites*, Research Report, 2006, http://hal.inria.fr/inria-00084202/en/.

[50] O. FESTOR, M. BURGESS, V. CRIDLIG, R. SZUMAN, E. LUPU, G. PAVLOU, J. SCHOENWAELDER. *Deliverable D6.1 - Open source support & joint software development interim report*, EMANICS FP6 NOE-026854, Contract Report, 2006, http://hal.inria.fr/inria-00113051/en/.

[51] O. FESTOR, M. BURGESS, G. DREO, G. PAVLOU, A. PRAS, J. SERRAT, J. SCHOENWAELDER, R. STATE, B. STILLER. *EMANICS Quaterly Management Report #2 : April-June 2006*, EMANICS, Contract Report, 2006, http://hal.inria.fr/inria-00109477/en/.

[52] O. FESTOR, M. BURGESS, G. DREO, G. PAVLOU, A. PRAS, J. SERRAT, J. SCHOENWALDER, R. STATE, B. STILLER. *EMANICS Quaterly Management Report #3 : July-September 2006*, EMANICS, Contract Report, 2006, http://hal.inria.fr/inria-00109469/en/.

[53] O. FESTOR, M. BURGESS, G. DREO, G. PAVLOU, A. PRAS, J. SERRAT, J. SCOENWALDER, R. STATE, B. STILLER. *EMANICS - Quaterly Management Report #1*, Contract Report, 2006, http://hal.inria.fr/inria-00109480/en/.

[54] O. FESTOR, S. D'HAESSELEER, S. FRÉNOT, H. ABDELNUR, V. CRIDLIG. *D B3.4 - Specification of Residential Gateway configuration*, IST MUSE, Contract Report, 2006, http://hal.inria.fr/inria-00113085/en/.

[55] O. FESTOR, G. DREO RODOSEK, F. EYERMANN, B. GAJDA, J. SCHOENWALDER, J. SERRAT, R. STATE. *D2.1 - Virtual Laboratory Integration Report*, EMANICS NoE, Contract Report, 2006, http://hal.inria.fr/inria-00113057/en/.

[56] J. FRANÇOIS. *Analyse comparative de méthodes de capture de traces d'attaques*, Internship Report, 2006, http://hal.inria.fr/inria-00112114/en/.

[57] D. LARREY, L. RODIER. *Géolocalisation par WiFi*, Research Report, 2006, http://hal.inria.fr/inria-00112186/en/.

[58] C. LEVOINTURIER. *Impact du modèle de comportement dans les réseaux pair à pair : une approche multi-agents*, Internship Report, 2006, http://hal.inria.fr/inria-00112567/en/.

[59] R. STATE, O. FESTOR. *Malware: A future framework for Device, Network and Service Management*, Research Report, 2006, http://hal.inria.fr/inria-00111987/en/.

References in notes

[60] 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.