INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Madynes

Management of Dynamic Networks and Services

Nancy - Grand Est

THEME COM

Activity Report

2007

Table of contents

1. Team

MADYNES is a project group of the LORIA (UMR 7503) laboratory, joint lab 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 2006 to December 31th, 2007.

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. Until 30/08/2007]
Caroline Suter [Project Assistant, INRIA. Since 1/10/2007]

INRIA Staff

Radu State [Researcher Associate (CR) INRIA]

University Staff

Laurent Andrey [Associate Professor, Nancy 2 University. On sabbatical at INRIA until 1/09/2007]
Rémi Badonnel [[Associate Professor, ESIAL, Henri Poincaré - Nancy 1 University, since 1/01/2007]
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]

Project Technical Staff

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

Ph.D. Students

Abelkader Lahmadi [Industrial grant, 3rd year]
Mohamed Nassar [MEN grant, 2nd year]
Humberto Jorge Abdelnur [Industrial grant with regional co-sponsorship, 2nd year]
Jérôme François [CNRS BDI grant with regional co-sponsorship, 1st year]
Cristian Popi [Industrial grant with regional co-sponsorship, 1st year]
Thibault Cholez [Industrial grant with regional co-sponsoship. Since 1/10/2007]
Julien Siebert [MADYNES-MAIA cooperation. Industrial grant with regional co-sponsoship. Since 1/10/2007]
Tom Leclerc [Industrial grant with regional co-sponsoship. Since 1/10/2007]

Invited Researchers

Omar Cherkaoui [Professor, UQAM. From 1/05/2007 to 30/08/2007]

Student Interns

Thibault Cholez [Ms Degree Internship, Nancy University. From 1/02/2007 to 30/08/2007]
Anca Ghitescu [Ms Degree Internship, Technical University Hamburg-Harburg, Germany. From 1/01/2007 to 1/03/2007]
Tom Leclerc [Ms Degree Internship, Nancy University. From 1/02/2007 to 30/08/2007]
Nataraj Mocherla [BsC Degree Internship, IIT. From 1/02/2007 to 30/06/2007]
Julien Siebert [Ms Degree Internship, Nancy University. From 1/02/2007 to 30/06/2007]
Livu Cristi Stefan [BsC Degree Internship, University of Pitesti. From 1/02/2007 to 30/04/2007]
Gérard Wagener [Ms Degree Internship, Nancy University. From 1/02/2007 to 30/08/2007]

2. Overall Objectives

2.1. Introduction

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

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

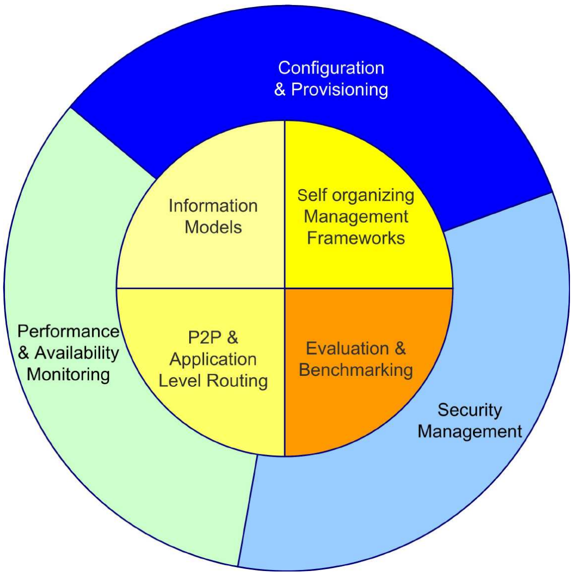
Configuration & Provisioning
Information Models
Self organizing Management Frameworks
Performance & Availability Monitoring
P2P & Application Level Routing
Evaluation & Benchmarking
Security Management

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 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.

2.2. Highlights of the year

The highlight of 2007 is the impact of our work on the design of new models and methods for stateful fuzzing and its application to Voice Over IP networks. The full model The method implemented in the KIF software tool was succesfully applied to all Voice over IP devices available to the team and major vulnerabilities were discovered for all tested devices, leading to numerous ethical disclosures and world-wide recognition of the power and of our approach and knowledge of the team. More than 1000 sites did/do reference our work on the web in 2007.

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

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

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.

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. Modeling 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 today’s 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 assessment. 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:

- Voice over IP networks,
- peer-to-peer infrastructures.
- ambiant environments.

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). The software is distributed under the LGPL licence as a SourceForge project at http://jdukebox.sourceforge.net/.

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 and 2007 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...). New attacks based on the Neighbor Discovery Protocol and Address Autoconfiguration (RFC 2461 and RFC 2462) have been identified and integrated in the tool. 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.

NDPMon comes along with a WEB interface acting as a GUI to display the informations gathered by the tool, and give an overview of all alerts and reports. Thanks to color codes, the WEB interface makes possible for the administrator to have an history of what happenned on his network and identify quickly problems. All the XML files used or produced by the daemon (neighbor cache, configuration file and alerts list) are translated in HTML via XSL for better readability. A statistic module is also integrated and gives informations about the discovery of the nodes and their type (MAC manufacturer repartition...).

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 several contributions have already been received. The tool has been ported to several Operating Systems (Linux, FreeBSD, OpenBSD, NetBSD and Mac OS X), and is integrated in FreeBSD ports at http://www.freebsd.org/cgi/cvsweb.cgi/ports/net-mgmt/ndpmon/. Binary distribution is also available for .deb and .rpm based Linux distributions. In 2007, we received funding from EMANICS to improve the packaging of the tool which has, thanks to this funding, been integrated in several GNU/Linux distributions.

5.4. rmidump

Participants: Laurent Andrey [contact], 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.

The two parts support a way to reverse rmi2 hashcodes to string function names. A first draft release of this utility will 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. Management benchmarking and performance models

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

In 2007, we focused the activity related to management performance evaluation on:

1. the study of the impact of instrumentation on applications,
2. the development of performance models for networks and services monitoring activities.

The first achievement is the development of a Java Management eXtension (JMX) conformant instrumentation for the Tjws web server. Several versions of this instrumentation have been designed to study the impact of the various integration models available when instrumenting java applications. The study has been conducted by using load injections and measurements on the instrumented application. Injection is twofold : one for the application plane using Jmeter a public domain tool and one for the management plane our “JMX benchmark” tool. This work is detailed in [53] and published in [26].

The second achievement comes as a conclusion for our past activity around performance evaluation of management frameworks. The main result is a model for the traditional management variable scrutation process. This model is based on a Repair Man model and several On/Off models. it has been published in [27] and some more general considerations in [25]. The PhD thesis of Abdelkader Lahmadi [7] covers all these results.

All these activities have been supported by the EMANICS network of excellence (work-package 7).

6.2. Fault Management in Autonomic Networks

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

In autonomic networks, fault detection is a management activity of crucial importance for increasing network availability and reliability. This activity is performed by the nodes themselves in a self-organized manner in order to identify and isolate pathological nodes. Our research activities in this context were focused on applying the concept of promised cooperation to different fault detection methods that we have previously proposed in [10]. This research work was done in cooperation with the research team of Prof. Mark Burgess at the Oslo University College - Norway, in the framework of the EMANICS network of excellence. Our objectives were (1) to determine to what extent promise theory can model the voluntary interactions among nodes during the detection process and (2) to identify possible limitations generated by our detection scheme. Promise theory approaches management from the viewpoint of uncertainty with realism rather than faith in compliance. It provides support for representing networks composed of entirely autonomous components.

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

Based on the analysis of the promise theoretical graph, we have observed that our detection mechanism is limited to exogenous factors (how the node perceives the others). This can be seen as a substantial advantage: the mechanism can detect a pathological node even if this node is not instrumented. However, we have shown through an extensive set of experiments that introducing an endogenous factor (how the node perceives itself) complementary to this exogenous factor can significantly improve performance. In that manner, network nodes can dynamically reduce the relative importance of their measurements during the detection process. We have quantified the benefits of this approach in terms of sensitivity and specificity. The results were published in [17].

6.3. Pervasive computing

Participants: Laurent Ciarletta [contact], Olivier Festor, Tom Leclerc, Julien Siebert.

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 two prospects:

- multi-models of these pervasive computing environments (including the users in the modelisation and the simulations). We have been focusing on the collaborative simulations of dynamic networks/elements, namely P2P (soon to be extended to adhoc networks) using agents to drive those simulations [48],
- State of the art on Service Discovery protocols [42] and contextual metrics in adhoc networks [46].

6.4. 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 already been 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 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 our work was motivated 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 SIP implementations. We have developed a conceptual approach and a fully operational prototype KIF which has discovered more then 30 vulnerabilities in widely used SIP stacks. These results were published in [15], [16]. We have followed an ethical disclosure policy and have actively supported the concerned vendors to fix the discovered vulnerabilities.

A second direction of research consisted in the development of conceptual models for VoIP intrusion detection. We proposed a holistic solution for VoIP security coupling the concept of VoIP honeypot with application specific monitoring. Preliminary research results were published in [24], [28], [30].

6.5. A Distributed and Adaptive Revocation Mechanism for Peer-to-Peer networks

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

Peer-to-Peer networks have proved their ability to gather and share a large amount of resources thanks to the collaboration of many individual peers. They are known to have many advantages compared to the client-server scheme: peer-to-peer networks scale better, the cost of the infrastructure is distributed and they are fault tolerant. However, peer-to-peer networks encounter several difficulties due to the important number of malicious peers. The lack of central authority and the individual behavior of the peers make it difficult for the peer-to-peer network to manage with them. Malicious peers can be classified in three main categories: the first one does not follow the peer-to-peer protocol and tries to make attacks, the second one shares malicious content (malware, pollution, illegal content), and the last one behaves in a selfish fashion. So, malicious behaviors really degrade the quality of service offered by peer-to-peer networks. In this context, peer-to-peer networks need a way to supervise the behaviors of their users.

We proposed a distributed and adaptive revocation mechanism [41] which does not need complex consensus and cryptographic mechanisms, hardly scalable. Our architecture is designed for structured P2P networks which have now proved their ability to be more efficient in their organization than unstructured ones and to provide more features. In our study, we focused on a specific structured network, .i.e. the KAD network. KAD is a part of the popular eMule and aMule file-sharing applications. It is based on the Kademlia protocol and is one of the widest deployed structured P2P network with millions simultaneous users.

Our revocation scheme is inserted in the core of the protocol, supervising the services provided by the P2P network and thus not a layered approach. The reputation needed to take decisions is provided by remote accounts based on the DHT used by structured P2P networks. For the time being, the evolution of the reputation concerns only the way the peers contribute to the network (regarding the bandwidth usage) to fight against the tragedy of the common problem. Each transaction between two peers is temporarily displayed on their blackboard to prove the evolution of the reputation. First analysis show that the resulting delays should not be sensed by the users. Moreover, the case study done to inventory the attacks tends to prove that the system itself is robust, as long as the allocation of a peer's ID is secured.

6.6. Autonomic IPv6 Management

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

We can observe that IPv6 deployment is slower than foreseen. The network administrators are indeed reluctant to deploy IPv6 because they do not master the protocol and all related issues. Therefore, one major challenge is to achieve a seamless transition from IPv4 to IPv6 and to avoid many problems, in terms of security or service outage. As the IPv4-IPv6 transition is a very complex operation, and can lead to the death of the network, there is a real need for a transition engine to ease the administrators' task; the ideal being a "one click" transition tool. For these reasons, and in the scope of our study we did in collaboration with CISCO on IPv6 network renumbering, we did define and implement a transition engine algorithm [37].

Our addressing mechanism is based on a logical representation of the network to assign. Virtual LAN are seen as different links in the graph, even if physically they are multiplexed on the same link. The network is thus represented as a graph. The root of this graph is the border router, which is the one interconnected with the ISP. That means that in case of multi-homing, we have one logical view of the network per border router. Weights are assigned to the links. Using these weights, all vertices calculate their shortest path to the root. The metric is then propagated from the leaves to the root, to determine the needs of each router.The assignation of the prefixes, contrary to the metric propagation, goes from the root to the leaves. The algorithm takes care of the route aggregation and tries to use as less address space as possible.

As a result, we obtain an addressing plan for the site, using the minimal number of /64 prefixes possible.

6.7. Worm based network management

Participants: Olivier Festor, Jérôme François, Radu State [contact].

The malware communication techniques are efficient and scalable. For instance, an attacker can control several thousands of machines by creating a botnet. Our research aims to propose a network management solution based on botnets. The first work focused on the potential performances and the practicability of such approach. We studied the botnet model that uses the Internet Relay Chat (IRC) protocol and an analytical model was proposed in [22]. To improve the results of this model, an extension was proposed in [21]. The results show that using an IRC botnet for doing network management provides good performances and is scalable because managing several thousand of computers with a limited delay is possible contrary to other management solutions.

Another family of botnets is based on the use of P2P protocols to do their signaling. Here, we studied different types of P2P botnets in order to evaluate their performances. We created two analytical models and did perform several simulations to evaluate the behavior of the metrics of interest to our study. Based on these simulations we were are able to evaluate what kind of botnet based management solution is best suited for a given management scenario. In fact depending on the number of devices to be managed or on the targeted applications, different types of botnet communications schemes are useful.

Since we studied and modeled the botnets, we are interested in providing new solution to detect them because this threat is one of the most dangerous on the Internet today. The current objective of our work is to improve the botnet detection and above all the botnet tracking solution. Thus, we not only want to simply detect a botnet but we also want to determine as many characteristics of them as possible. One of theses interesting characteristics is the size of the botnets i.e. the number of compromised hosts. The ultimate objective is to discover the location and identify the controller of the botnet.

6.8. Malware analysis

Participants: Gérard Wagener, Radu State [contact].

We have done work (joint work with Gérard Wagener and Alexandre Dulaunoy, Astra Luxembourg) on automated classification and analysis of malware. Our work is based on extracting a profile of the underlying behavior and classifying an unknown malware based on this profile. The extracted profile is obtained by recovering all system calls, and information theoretic measures are used for the classification. Our work addressed also the case of armored malware, where strong protection and anti-reverse engineering is used. We proposed an analysis method, where a virtualized and customized environment allows to learn the internal behavior of a piece of malware. This work needs to be extended towards more innovative analysis algorithms (for instance coding theory can error correction codes might be appropriate) and automated on demand virtual environments, that can be spawned on demand in order to analyze a piece of malware. The latter area of work will allow to leverage virtualized environments for capturing, analyzing and classifying unknown malware. The interest of such a work is to detect new offsprings (of an existing malware) or new and previously unknown pieces of malware.

7. Contracts and Grants with Industry

7.1. MUSE

Participants: Humberto Abdelnur, Frédéric Beck, Cristi Popi, 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. In 2007, we did implement the TR-69/Netconf gateway on top of the MADYNES Ensuite Netconf platform. The implementation has been fully intergrated in the MUSE testbed in the Alcatel-Lucent premises in Antwerpen in march 2007. A demonstration including a Netconf-based ACS (from MADYNES) managing TR-69 enabled gateways from Thomson was succesfully setup and transfer achieved to the project partners.

7.2. AIRNET

Participants: Olivier Festor [contact], Cristian Popi.

Dates June 2006 - May 2009

Partners LSR-IMAG (Leader), LIP6, Université Pierre et Marie Curie, Eurécom, LSIIT, INRIA (MADYNES), Division R&D de France Télécom, 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 investigation of distributed monitoring for mobile ad-hoc mesh-networks.

In 2007, we have elaborated a state of the art in MESH networks management [47] and we have designed a distributed monitoring scheme enabling network wide state to be collected over time and accessed by any management entity through a distributed hash table.

7.3. SARAH

Participants: Laurent Ciarletta [contact], Tom Leclerc, Julien Siebert.

Dates February 2007 - January 2010

Partners INRIA Lorraine (MADYNES), INRIA Rocquencourt (HIPERCOM) , LRI, LIP6, INT Ucopia, France Telecom R&D

SARAH is an ANR (Agence Nationale pour la Recherche, French National Research Agency) collaborative research project, in the area of Pervasive Computing. It aims at researching, implementing, experimenting and evaluating (a) novel hybrid ad hoc architecture(s) for the deployment of advanced multimedia services.

These services will be secured and use (geo)localized information provided by service discovery protocols and follow Pervasive Computing requirements :

- ubiquitous availability,
- context awareness,
- self adaptation to the users' needs (the technology adapts and is available to provide services to the user and not the other way around)
- disappearing computing (discreetly, almost naturally embedded in our daily environment)
- ease of use.

Therefore it is not only necessary to extend the reach, the availability and the functionality of applications and services but also to ubiquitously offer them in the most secure and easy (natural) possible way.

We contribute to the following activities of the project :

- Context aware service discovery for advanced services in ad hoc network. There, we will investigate the technologies and metrics needed in the project for service discovery protocols and the subsequent needs in the management plane.
- simulation, prototypes, demo and evaluation of proof of concepts services and environment : in order to develop, evaluate and validate the overall project solutions, we will work both on simulations and on real-world implementations.

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.

7.4. CISCO

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

Dates January 2006 - Juillet 2007

Partners CISCO Systems

Starting on the 1st of January 2006, with Cisco sponsorship, we continued the study on IPv6 renumbering, while focusing on the network 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 to complete the definition of a generic firewall update framework [36] that implements the algorithms which automate the rules rewriting and the configuration of firewall during a network renumbering and also the service that interacts with the remote firewalls to actually push/pull the configuration to/from the firewalls.

While IPv6 is slowly being deployed in networks, and begins to be used widely by the ISPs, especially for management issues, the need for monitoring and managing such networks grows at the same time. We proposes a solution for monitoring the Neighbor Discovery Protocol, we called NDPMon. Basically, the idea is to implement an IPv6 version of ArpWatch. But, as the Neighbor Discovery Protocol is more complex than ARP, some other functionalities are required [19], [51].

Knowing only the IP address of a host is mandatory but not sufficient to perform all the monitoring management operations on a system. Determine the type of an operating system related to a device can help to find how to access to its services and/or to its data and which are its potential vulnerabilities. So we used the Neighbor Discovery Protocol to perform OS Fingerprinting in IPv6 [38] and extend the NDPMon monitoring tool we developed.

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

In october 2007, Olivier Festor was nominated co-chair of IFIP WG6.6.

We actively participate to the Internet Research Task Force (IRTF) Network Management Research Group (NMRG). In 2007, we did participate to the 23rd NMRG meeting held in Enschede, The Netherlands in Twente. In 2007, we did co-author a position paper on challenges established during the joint EMANICS NMRG meeting in Utrecht in 2006 [14].

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.

8.2. 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. In 2007, Olivier Festor gave a tutorial entitled: The Management plane in Autonomc Networks.

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.

8.3. Guest Researchers

Omar Cherkaoui, Professor at UQAM spent 4 months in the team. He did work with Mohamed Nassar on statistical models for intrusion detection in Voice Over IP and start an activity on vitalization techniques for networks and their management in the team. One joint project was submitted to the EC as part of the second call of FP7 on this topic.

Rémi Badonnel spent 6 months at Oslo University Colleague in the team of Mark Burgess. There he worked on the coupling of probabilistic management with promise theory.

9. Dissemination

9.1. Program committees and conference organization

Radu State was TPC Co-chair of the following events in 2007 : IEEE MONAM 2007 Monitoring and Attack Mitigation 2007, Toulouse, France (with Ph. Owezarski); First International Workshop on Cyber-Fraud (Cyber-Fraud), Silicon Valley, 2007. USA (with T. Chen), SAR-SSI 2007 Securité, Architecture, Réseaux 2007, Anency, France (with Alexis Bonnecaze and Jean Leneutre). He was Poster Co-Chair for IEEE/IFIP IM 2007: 10 th. IEEE/IFIP International Conference on Integrated Network Management. IM2007, Muenchen, Germany.

Radu State was technical program committee member for : the 10 th. IEEE/IFIP International Conference on Integrated Network Management. IM2007, Muenchen, Germany, IPTCOMM (Principles, Systems and Applications of IP Telecommunications), 2007, New York, USA, and the IEEE/IFIP DSOM 2007, the 18 th IEEE/IFIP Workshop on Distributed Systems Management and Operations.

Isabelle Chrisment Steering is member of the steering committee of SAR 2007. She was member of the following technical program committees : SAR 2007, NOTERE 2007, MonAM 2007, EUNICE 2007, AIMS 2007 (where she also co-chaired the Tutorial track).

In 2006, Olivier Festor was member of the following program committees: IFIP/IEEE IM'2007 (where he also acted as workshop co-chair), IFIP/IEEE DSOM'2007, ACM AIMS'2007, GRES'2007.

Olivier Festor is also member of the Board of Editors of the Journal of Systems and Network Management and reviewed 32 papers for several international conferences and journals in 2005.

9.2. Teaching

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

9.3. Tutorials, invited talks, panels, presentations

In addition to the presentation of all papers published in conferences in 2007, the team members made the following presentations:

- Olivier Festor gave a tutorial on Management and Autonomic Networks at the RESCOM summer school.
- Olivier Festor gave a keynote talk on Management and Autonomic Networks at the at the University of Delaware.
- Radu State gave an invited talk on Voice Over IP Fuzzing at the University of Delaware.
- Humberto Abdelnur Gave a presentation on stateful fuzzing at the University of Delaware.

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

9.4. Commissions

Olivier Festor was member of the European Commission panel for the first FP7 call entitled “Network of the Future”. He also served as an expert for the european ERC program.

Both Laurent Andrey and Isabelle Chrisment served as experts for the OSEO-ANVAR agency.

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

- Abdelkader Lahmadi, Ph.D. in Computer Science from Nancy 2 University France, *Performances des fonctions et architectures de supervision de réseaux et de services*, Laurent Andrey, Omar Cherkaoui (reviewer), Olivier Festor, Jean-François Mary, Aiko Pras, Guy Pujolle (reviewer), december 2007.

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

- Mohamed AIT ALI, Ph.D. in Computer Science from Nancy Université. title: *Amélioration de la Mesure de la Bande Passante dans un Réseau Basé sur IP*, Committee: Ph. Owezarski (reveiwer), V. Vèque (reviewer), O. Festor, B. Thirion (commitee president), F. Lepage, Th. Divoux, November 2007.
- Nader M BAREK, Ph.D. in Computer Science from Université Bordeaux 1. title: *Autonomie dans les réseaux : Négociations du niveau de service de bout en bout dans un framework de gestion autonome*, Committee: F. Krief, A. Karmouch (reviewer), G. Pujolle (reviewer), R. Castanet, O. Festor, A. Cotton, october 2007.
- Eun-Young KANG, Ph.D. in Computer Science from the Henri Poincaré University Nancy 1. Title: *Abstraction booléennes pour la vérification des systèmes temps-réel*, Committee: Christian Attiogbé (reviewer), Jean-Paul Bahsoun (reviewer), Jean-Paul Bodeveix, Isabelle Chrisment (president), Yamine Ait-Ameur, Dominique Méry, Stephan Merz, November 2007.
- Heinrich HOERDEGEN, Ph.D. in Computer Science from the Henri Poincaré University Nancy 1. Title: *Vérification des protocoles cryptographiques : Comparaison des modèles symboliques avec une application des résultats — Étude des protocoles récursifs*, Committee: Gaétan Hains (reviewer), Ralf Treinen (reviewer), Isabelle Chrisment, Véronique Cortier, Fran cois Laroussinie, Michael Rusinovitch, November 2007.
- Samuel GALICE, Ph.D. in Computer Science from the INSA, Lyon. Title: *Modèle dynamique de sécurité pour réseaux spontanés*, Committee: Al Agha Khaldoun (reviewer), Valérie Issarny (reviewer), Isabelle Chrisment, Daniel Le Métayer, Stéphane Ubéda, Marine Minier, November 2007.

Team members reviewed the following Ph.D. thesis:

- Issam AIB, Ph.D. in Computer Science from Université Pierre et Marie Curie - Paris 6. title: *Une approche orientée buts d’affaires pour l’optimisation des politiques*, Committee: G. Pujolle, R. Boutaba, G. Pavlou (reviewer), O. Festor (reviewer), O. Cherkaoui, P. Sens, C. Bartolini, july 2007.
- Yohann THOMAS, Ph.D. in Computer Science from ENST Bretagne. title: *Policy-based Response to Intrusions Through Context Activation*, Committee: O.Festor (reviewer), C. Kruegel (reviewer), M Ducasse, F. Cuppens, H. Debar, N. Cuppens, O. Paul, P. Radja, november 2007.
- Hélia POUYLLAU, Ph.D. in Computer Science from Université Rennes 1. title: *Algorithmes distribués pour la négociation de contrats de qualité de service dans les réseaux multi-domaines*, Committee: G.v. Bochman (reveiwer), O. Festor (reviewer), J-C. Grégoire, B. Tuffin, A. Aghasaryan, S. Haar, december 2007.
- Yvan ROYON, Ph.D. in Computer Science from INSA de Lyon. title: *Environnements d’exécution pour passerelles domestiques*, Committee: S. Frénot, S. Ubéda, O. Festor (reviewer), G. Muller (reviewer), D. Donsez, G. Grimaud, N. Le Sommer, december 2007.

- Hani Ragab HASSEN, Ph.D. in Computer Science from the University of Technology, Compiègne. Title: *Key Management for Content Acces Control in Hierarchical Environments*, Committee: Bernard Cousin (reviewer), Isabelle Chrisment (reviewer), Ahmed Serhrouchni, Abdelmadjid Bouabdallah, Hatem Bettahar, December 2007.

MADYNES members were members of the following Habilitation Degree commissions:

- Matthieu LATAPY, Habilitation Degree in Computer Science from Université Pierre et Marie Curie - Paris 6. Title: *Grands graphes de terrain - mesure et métrologie, analyse, modélisation, algorithmique*, Committee : P. Abry, G. Ausiello, F. Baccelli, V. Blondel, O. Festor, E. Fleury, P. Gallinari, M. Habib, november 2007.
- Damien MAGONI, Habilitation Degree in Computer Science from Université Louis Pasteur Strasbourg. Title: *Topologies de L'Internet : des Routeurs aux Réseaux Recouvrants*, Committee : D. Bechmann, J-F. Dufourd, S. Fdida, O. Festor, M. Freire, P. Lorenz, december 2007.

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

Doctoral dissertations and Habilitation theses

[7] A. LAHMADI. *Performances des fonctions et architectures de supervision de réseaux et de services*, Ph. D. Thesis, Université de Nancy 2, december 2007.

Articles in refereed journals and book chapters

[8] R. Badonnel, R. State, O. Festor. *A Probabilistic Approach for Managing Mobile Ad-Hoc Networks*, in "IEEE Transactions on Network and Service Management", vol. 3, 2007, http://hal.inria.fr/inria-00153555/en/.

[9] R. Badonnel, R. State, O. Festor. *Management of Ad-Hoc Networks*, in "Handbook of Network and System Administration", J. Bergstra, M. Burgess (editors), Elsevier B.V. All rights reserved, 2007, http://hal.inria.fr/inria-00153547/en/.

[10] R. Badonnel, R. State, O. Festor. *Self-Configurable Fault Monitoring in Ad-Hoc Networks*, in "Ad-Hoc Networks", 2007, http://hal.inria.fr/inria-00153604/en/.

[11] M. S. Bouassida, N. Chridi, I. Chrisment, O. Festor, L. Vigneron. *Automated Verification of a Key Management Architecture for Hierarchical Group Protocols*, in "Annals of Telecommunications", A paraître, 2007, http://hal.inria.fr/inria-00167824/en/.

[12] M. S. Bouassida, I. Chrisment, O. Festor. *Gestion de clés dans les réseaux ad hoc*, in "La sécurité dans les réseaux sans fil et mobiles Réseaux et Télécoms IC2", Réseaux et Télécoms IC2, vol. 3, Lavoisier-Hermes science, 2007, p. 139-181, http://hal.inria.fr/inria-00167822/en/.

[13] M. S. Bouassida, I. Chrisment, O. Festor. *Group Key Management in MANETs*, in "International Journal of Network Security", To appear, vol. 6, 2008, p. 67-79, http://hal.inria.fr/inria-00167843.

[14] A. Pras, J. Schoenwaelder, M. Burgess, O. Festor, G. Martinez Perez, R. Stadler, B. Stiller. *Key Research Challenges in Network Management*, in "IEEE Communications Magazine", vol. 45, 2007, http://hal.inria.fr/inria-00192236/en/.

Publications in Conferences and Workshops

[15] H. Abdelnur, O. Festor, R. State. *KiF: A stateful SIP Fuzzer*, in "1st International Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm), New York États-Unis d'Amérique", ACM SIGCOMM, Columbia University, 07 2007, http://hal.inria.fr/inria-00166947/en/.

[16] H. Abdelnur, R. State, I. Chrisment, C. Popi. *Assessing the security of VoIP Services*, in "The Tenth IFIP/IEEE International Symposium on Integrated Network Management - IM 2007 10th IFIP/IEEE International Symposium on Integrated Network Management, Munich/Germany", ISBN : 1-4244-0799-0/http://www.comsoc.org, IEEE Communication Society, 05 2007, p. 373-382, http://hal.inria.fr/inria-00148363/en/.

[17] R. Badonnel, M. Burgess. *Fault Detection in Autonomic Networks using the Concept of Promised Cooperation*, in "18th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM'07, MANWEEK'07), San José, CA États-Unis d'Amérique", Springer-Verlag Lecture Notes in Computer Science (LNCS), IEEE Communications Society, 10 2007, http://hal.inria.fr/inria-00167717/en/.

[18] R. Badonnel, R. State, I. Chrisment, O. Festor. *A Management Platform for Tracking Cyber Predators in Peer-to-Peer Networks*, in "The Second International Conference on Internet Monitoring and Protection - ICIMP 2007, Santa Clara, CA/USA", 2007, http://hal.inria.fr/inria-00153620/en/.

[19] F. BECK, T. CHOLEZ, O. FESTOR, I. CHRISMENT. *Monitoring the Neighbor Discovery Protocol*, in "The Second International Workshop on IPv6 Today - Technology and Deployment - IPv6TD 2007, Guadeloupe/French Caribbean Guadeloupe", 03 2007, http://hal.inria.fr/inria-00153558/en/.

[20] J. FRANÇOIS, R. STATE, O. FESTOR. *Activity Monitoring for large honeynets and network telescopes*, in "The Second International Conference on Internet Monitoring and Protection, San Jose États-Unis d'Amérique", IEEE/IARIA, 2007, http://hal.inria.fr/inria-00172053/en/.

[21] J. FRANÇOIS, R. STATE, O. FESTOR. *Botnets for scalable management*, in "18th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM'07, MANWEEK'07) Managing Virtualization of Networks and Services Lecture Notes in Computer Science, San José États-Unis d'Amérique", Lecture Notes in Computer Science, vol. 4785, Springer, 10 2007, http://hal.inria.fr/inria-00170425/en/.

[22] J. FRANÇOIS, R. STATE, O. FESTOR. *Malware models for network and service management*, in "First International Conference on Autonomous Infrastructure, Management and Security, AIMS Inter-Domain Management Lecture Notes in Computer Science, Oslo Norvège", Lecture Notes in Computer Science, vol. 4543, Springer, 2007, p. 192-195, http://hal.inria.fr/inria-00168415/en/.

[23] J. FRANÇOIS, A. EL-ATAWY, E. AL SHAER, R. BOUTABA. *A collaborative approach for proactive detection of distributed denial of service attacks*, in "IEEE Workshop on Monitoring, Attack Detection and Mitigation - MonAMÕ2007, Toulouse France", 2007, http://hal.inria.fr/inria-00188020/en/.

[24] B. KARPAGAVINAYAGAM, R. STATE, O. FESTOR. *Monitoring Architecture for Lawful Interception in VoIP Networks*, in "Second International Conference on Internet Monitoring and Protection - ICIMP 2007, Silicon Valley États-Unis d'Amérique", 07 2007, http://hal.inria.fr/inria-00164420/en/.

[25] A. LAHMADI, L. ANDREY, O. FESTOR. *Modeling and Performance Evaluation of the Network and Service Management Plane*, in "Inter-Domain Management - First International Conference on Autonomous Infrastructure, Management and Security AIMS Lecture Notes in Computer Science, Oslo Norvège", A. K. BANDARA, M. BURGESS (editors), Lecture Notes in Computer Science, vol. 4543, Springer, 2007, p. 156-159, http://hal.inria.fr/inria-00169010/en/.

[26] A. LAHMADI, A. GHITESCU, L. ANDREY, O. FESTOR. *On the Impact of Management Instrumentation Models on Web Server Performance: A JMX Case Study*, in "Inter-Domain Management, First International Conference on Autonomous Infrastructure, Management and Security AIMS Lecture Notes in Computer Science, Oslo Norvège", A. K. BANDARA, M. BURGESS (editors), Lecture Notes in Computer Science, vol. 4543, Springer, 06 2007, p. 1-12, http://hal.inria.fr/inria-00169007/en/.

[27] A. LAHMADI, A. LAURENT, F. OLIVIER. *Un modèle analytique pour l'évaluation de la supervision de réseaux et de services*, in "8ème Colloque Francophone de Gestion de Réseaux et de Services", 2007, http://hal.inria.fr/inria-00190899/en/.

[28] M. E. B. NASSAR, S. NICCOLINI, R. STATE, T. EWALD. *Holistic VoIP Intrusion Detection and Prevention System*, in "IPTCOMM 2007 Telecommunications in the Internet Age, New York États-Unis d'Amérique", Columbia University New York in Cooperation with ACM SIGCOMM, Columbia University New York in Cooperation with ACM SIGCOMM, 2007, p. 1-9, http://hal.inria.fr/inria-00169036/en/.

[29] M. E. B. Nassar, R. State, O. Festor. *IBGP confederation provisioning*, in "Autonomous infrastructure, management and security (AIMS 2007), Oslo Norvège", A. K. Bandara, M. Burgess (editors), Springer-Verlag Berlin, 06 2007, p. 25-34, http://hal.archives-ouvertes.fr/hal-00157302/en/.

[30] M. E. B. Nassar, R. State, O. Festor. *Voip Honeypot Architecture*, in "IM 2007 - Moving from Bits to Business Value 10th IFIP/IEEE International Symposium on Integrated Network Management, Munich, Germany", http://www.comsoc.org, IEEE Communications Society, IFIP/IEEE, 05 2007, p. 109-118, http://hal.inria.fr/inria-00149554/en/.

[31] R. State, V. Cridlig, O. Festor. *A model for checking consistency in access control policies for network management*, in "10th IFIP/IEEE International Symposium on Integrated Management (IM 2007), Munich Allemagne", IEEE (editor), IEEE, 2007, http://hal.inria.fr/inria-00172054/en/.

[32] R. State, M. Nassar, O. Festor. *BGP confederation provisioning*, in "Autonomous Infrastructure, Management and Security (AIMS 2007), Oslo Norvège", ACM (editor), ACM, 2007, http://hal.inria.fr/inria-00172057/en/.

Internal Reports

[33] H. Abdelnur, R. State, O. Festor. *Technical Report: Stateful Fuzzer*, Research Report, 2007, http://hal.inria.fr/inria-00141133/en/.

[34] R. Badonnel, M. Burgess, O. Fredy, D. Gonzalez, A. Hadjiantonis, I. Hochstatter, R. Koenig, E. Lupu, A. Malatras, K. Nowak, G. Pavlou, A. Pras, J. Rubio-Loyola, J. Schoenwaelder, J. Serrat, R. Stadler, T. Varma. *Next Generation Management Technologies and Approaches to Support Autonomic Management*, Contrat, 2007, http://hal.inria.fr/inria-00170552/en/.

[35] F. Beck. *NetFlow, RMON and Cisco-NAM deployment*, Technical Report, n^{O} RT-0343, INRIA, 2007, http://hal.inria.fr/inria-00169995/en/.

[36] F. Beck, I. Chrisment, O. Festor. *IPv6 Renumbering - Security and Monitoring. D3.1 - Monitoring Framework*, Contrat, 2007, http://hal.inria.fr/inria-00170636/en/.

[37] F. Beck, O. Festor, I. Chrisment. *IPv4 to IPv6 Transition Engine*, Technical Report, n^{O} RT-0344, INRIA, 2007, http://hal.inria.fr/inria-00169993/en/.

[38] F. Beck, O. Festor, I. Chrisment. *IPv6 Neighbor Discovery Protocol based OS fingerprinting*, Technical Report, n^{O} RT-0345, INRIA, 2007, http://hal.inria.fr/inria-00169990/en/.

[39] M. Burgess, G. Dreo Rodosek, O. Festor, G. Pavlou, A. Pras, J. Schoenwaelder, J. Serrat, R. Stadler, R. State, B. Stiller. *Quarterly Management Report #5*, Contrat, 2007, http://hal.inria.fr/inria-00170555/en/.

[40] M. Burgess, G. Dreo Rodosek, O. Festor, G. Pavlou, A. Pras, J. Schoenwaelder, J. Serrat, B. Stiller. *Quarterly Management Report #6*, Contrat, 2007, http://hal.inria.fr/inria-00170556/en/.

[41] T. Cholez. *Conception de mécanismes de révocation et de réputation dans un environnement pair-à-pair*, Stage, 2007, http://hal.inria.fr/inria-00168337/en/.

[42] L. Ciarletta, T. Leclerc, G. Pujolle, P. Borras, S. Gashti. *Etude des protocoles de découverte de service dans le cadre des réseaux adhoc*, Contrat, 2007, http://hal.inria.fr/inria-00172067/en/.

[43] O. Festor, F. Beck, M. Burgess, E. Lupu, G. Pavlou, J. Schoenwaelder, R. Szuman, R. Stadler, V. Cridlig. *Open Source Support and Joint Software Development : Final Report*, Contrat, 2007, http://hal.inria.fr/inria-00170548/en/.

[44] O. Festor, F. Beck, G. Dreo Rodosek, O. Festor, A. Pras, J. Schoenwaelder, J. Serrat, R. State, B. Stiller. *Virtual Laboratory Integration Report*, Contrat, 2007, http://hal.inria.fr/inria-00170549/en/.

[45] O. Festor, M. Burgess, G. Dreo Rodosek, G. Pavlou, A. Pras, J. Schoenwaelder, J. Serrat, R. State, B. Stiller. *Quarterly Management Report #4*, Contrat, 2007, http://hal.inria.fr/inria-00170554/en/.

[46] T. Leclerc. *Métriques contextuelles et outils d'évaluation pour la découverte de service dans les réseaux hybrides*, Travaux universitaires, 2007, http://hal.inria.fr/inria-00172070/en/.

[47] C. Popi, O. Festor. *State of the art in Wireless Mesh Networks - delivrable L3.01 - RNRT project "Airnet"*, Research Report, 2007, http://hal.inria.fr/inria-00147944/en/.

[48] J. Siebert. *Impact du comportement des utilisateurs dans les réseaux pair-à pair, modélisation et simulation multi-agents*, Travaux universitaires, 2007, http://hal.inria.fr/inria-00172068/en/.

[49] R. State, L. Andrey, O. Festor, J. Schoenwaelder, A. Pras, G. Pavlou, K. Nowak, T. Balanescu. *Deliverable D7.2 - Final report on benchmarking of management protocols*, Contrat, 2007, http://hal.inria.fr/inria-00191889/en/.

[50] G. Wagener. *Paradigmes d'Analyse de Programmes Malicieux*, Technical Report, 2007, http://hal.inria.fr/inria-00186915/en/.

Miscellaneous

[51] F. Beck, T. Cholez, O. Festor, I. Chrisment. *Supervision IPv6 - Applications Spécifiques - NDPMon*, 2007, http://hal.inria.fr/inria-00170761/en/.

[52] O. Festor. *The Management Plane in Autonomic Networks*, 2007, http://hal.inria.fr/inria-00170557/en/.

[53] A. Ghitescu. *Performance evaluation of JMX Models*, 2007, http://hal.inria.fr/inria-00168520/en/.

[54] R. State, C. Stefan. *An Asterisk monitoring infrastructure based on Nagios*, 2007, http://hal.inria.fr/inria-00172050/en/.