IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2012

Project-Team MADYNES

Management of dynamic networks and services

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
Nancy - Grand Est

THEME
Networks and Telecommunications

Table of contents

Project-Team MADYNES

Keywords: Ambient Computing, Monitoring, Peer-to-peer, Security, Self-management

Creation of the Project-Team: February 01, 2004 .

1. Members

Research Scientist

Olivier Festor [Team Leader, Research Director (DR) 20% of his time, Inria, HdR]

Faculty Members

Isabelle Chrisment [Professor, TELECOM Nancy - Université de Lorraine, HdR]
Laurent Andrey [Associate Professor, IUT Charlemagne - Université de Lorraine]
Rémi Badonnel [Associate Professor, TELECOM Nancy - Université de Lorraine]
Laurent Ciarletta [Associate Professor, ENSMN - Université de Lorraine]
Abdelkader Lahmadi [Associate Professor, ENSEM - Université de Lorraine]
Emmanuel Nataf [Associate Professor, IUT Charlemagne - Université de Lorraine]
André Schaff [Professor, TELECOM Nancy - Université de Lorraine, HdR]
Ye-Qiong Song [Professor, ENSEM - Université de Lorraine, HdR]
Thomas Silverston [Associate Professor, Faculté des Sciences et Technologies - Université de Lorraine, HdR]

Engineers

Alexandre Boeglin [Engineer, Industrial grant]
Moutie Chehaider [Engineer, Inria grant (-12/2012)]
Adrien Guenard [Research Engineer, Industrial grant (-12/2012)]
Bilel Nefzi [Research Engineer, Industrial grant (04/2012 - 09/2012)]
Yannick Presse [Research Engineer, Industrial grant (10/2012-)]
Bilel Saadallah [Research Engineer, Industrial grant (03/2012-)]

PhD Students

Sheila Becker [Co-tutelle with University of Luxembourg (-10/2012)]
Martin Barrere [Industrial grant (01/2011-)]
Oussema Dabbebi [Industrial grant (10/2009-10/2012)]
César Bernardini [01/2012-)]
François Despaux [10/2011-)]
Patrick-Olivier Kamgueu [6/2012-)]
Juan Pablo Timpanaro [Industrial grant with regional co-sponsoship (01/2010-)]

Administrative Assistant

Céline Simon [Project Assistant, Inria]

2. Overall Objectives

2.1. Overall Objectives

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

The project develops applied research activities in the following areas:

- **Autonomous Management**:
  - the design of models and methods enabling **self-organization and self-management** of networked entities and services,
  - the evaluation of management architectures based on **peer-to-peer and overlay principles**,
  - the investigation of novel approaches to the representation of **management information**,
  - the modeling and **performance evaluation** of dynamic networks.
- **Functional Areas** instantiate autonomous management functions:
  - the **security plane** where we focus on building closed-loop approaches to protect networking assets,
  - the **service configuration** where we aim at providing solutions covering the delivery chain from device discovery to QOS-aware delivery in dynamic networks,
  - **monitoring** where we aim at building solutions to characterize and detect unwanted service behavior.

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 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 has 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 Fault, Configuration, Accounting, Performance and Security 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.

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 modeling 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 dynamic networks

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).

MADYNES addresses this problem from multiple viewpoints: communication patterns, processing and memory resources consumption. Our goal is to provide management patterns combining optimized management technologies so as to optimize the resources consumed by the management activity imposed by the operating environment while ensuring its efficiency in large dynamic networks.

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 establishing 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 configurations 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 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:

- sensor networks,
- peer-to-peer infrastructures,
- information centric networks,
- ambiant environments.

5. Software

5.1. SecSIP

Participants: Abdelkader Lahmadi [contact], Olivier Festor.

SecSip [1] is developed by the team to defend SIP-based (The Session Initiation Protocol) services from known vulnerabilities. It presents a proactive point of defense between a SIP-based network of devices (servers, proxies, user agents) and the open Internet. Therefore, all SIP traffic is inspected and analyzed against authored Veto specification before it is forwarded to these devices. When initializing, the SecSIP runtime starts loading and parsing authored VeTo blocks to identify different variables, event patterns, operations and actions from each rule. Veto is a generic declarative language for attack patterns specification. SecSIP implements an input and output layer, to capture, inject, send and receive SIP packets from and to the network. Intercepted packets are moved to the SIP Packet parser module. The main function of this module is to extract different fields within a SIP message and trigger events specified within the definition blocks. During each execution cycle when a SIP message arrives, the SecSIP runtime uses a data flow acyclic graph network to find definition matching rules and triggers defined events. The paired events in each operator node are propagated over the graph until a pattern is satisfied. When the pattern is satisfied, the respective rule is fired and the set of actions is executed.

SecSIP is freely available on the Internet. It was extended to support new protocols in the area of SCADA systems in 2012.

5.2. NDPMon

Participants: Isabelle Chrisment, Olivier Festor [contact].

[1] http://secsip.gforge.inria.fr/doku.php

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 Auto-configuration (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 happened 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 distribution ...).

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 open source community is now established for the tool which has distributions for several Operating Systems (Linux, FreeBSD, OpenBSD, NetBSD and Mac OS X). It is also integrated in FreeBSD ports at http://www.freebsd.org/cgi/cvsweb.cgi/ports/net-mgmt/ndpmon/. Binary distributions are also available for .deb and .rpm based Linux flavors.

In 2012, the software underwent a complete reshaping thanks to a substantial support from the High Security Lab which dedicated us 6 months of research engineer.

6. New Results

6.1. Android Security

Participants: Olivier Festor, Abdelkader Lahmadi [contact].

Android-based devices include smartphones and tablets that are now widely adopted by users because they offer a huge set of services via a wide range of access networks (WiFi, GPRS/EDGE, 3G/4G). Android provides the core platform for developing and running applications. Those applications are available to the users over numerous online marketplaces. These applications are posted by developers, with little or no review process in place, leaving the market self-regulated by users. This policy generates a side-effect where users are becoming targets of different malicious applications which the goal is to steal their private information, collect all kind of sensitive data via sensors or abusing granted permissions to make surtaxed calls or messages. To address this security issue, monitoring the behaviour of running applications is a key technique enabling the identification of malicious activities.

During 2012, we have designed and developed a monitoring framework integrating observed network and system activities of a running application. We have developed an embedded NetFlow probe running on android devices to export observed network flow records observed to a collection point for their processing. Our embedded probe includes a new set of IPFIX information elements that we have designed [36] to encapsulate location information within exported flows using the IPFIX protocol.

We have also developed an embedded logging probe that exports available system logs to a collection point. The logs are then centrally processed and correlated with observed network flow records to extract an accurate behavior of an application including its network and in-device activities.

Our monitoring framework is different from available proposed solutions since we build a dynamic model to infer the running behavior of an Android application. This technique allows us to identify patched applications where a malicious activity has been added, cloned applications where the observed behavior is different from the expected behavior and privacy leaks where an application is contacting unexpected services.

6.2. Sensor networks monitoring

Participants: Alexandre Boeglin, Laurent Ciarletta, Olivier Festor, Abdelkader Lahmadi [contact], Emmanuel Nataf, Bilel Saadallah.

Low Power and Lossy Networks (LLNs) are made of interconnected wireless devices with limited resources in terms of energy, computing and communication. The communication channels are low-bandwidth, high loss rate and volatile wireless links subject to failure over time. They are dynamic and the connectivity is limited and fluctuant over time. Each node may loss frequently its connectivity with its neighborhood nodes. In addition, link layer frames have high constrains on their size and throughput is limited. These networks are used for many different applications including industrial automation, smart metering, environmental monitoring, homeland security, weather and climate analysis and prediction. The main issue in those networks is optimal operation combined with strong energy preservation. Monitoring, i.e the process of measuring sampled properties of nodes and links in a network, is a key technique in operational LLNs where devices need to be constantly or temporally monitored to assure their functioning and detect relevant problems which will result in an alarm being for- warded to the enterprise network for analysis and remediation.

During the year 2012, we developed novel approaches for the monitoring of LLNs. We developed and designed a novel algorithm and a supporting framework [18] that improves a poller-pollee monitoring architecture. We empower the poller-pollee placement decision process and operation by exploiting available routing data to monitor nodes status. In addition, monitoring data is efficiently embedded in any messages flowing through the network, drastically reducing monitoring overhead. Our approach is validated through both simulation, implementation and deployment on a 6LoWPAN-enabled network. Both simulations and large-scale testbed experiments assess the efficiency of our monitoring scheme. Results also demonstrate that our approach is less aggressive and less resource consuming than its competitors.

We developed a first fully operational CCNx stack [40] on a wireless sensor network. We implemented CCNx as a native C experimental extension of Contiki, an operating system dedicated to Internet of Things applications. Our extension [33] is based on the reference implementation of CCNx modified to run as a network driver on top of different available MAC protocols implementations in Contiki. Our goal is to design a monitoring and configuration framework that benefits from the content-centric approach to efficiently collect desired management content and apply in-network processing functions for nodes configuration and monitoring. This includes extending naming schema with monitoring oriented processing functions, optimizing data interests to minimize the communication overhead.

6.3. Management and monitoring of P2P networks

Participants: Isabelle Chrisment [contact], Olivier Festor, Juan Pablo Timpanaro.

In 2012, we have addressed operation, monitoring and security issues on several P2P target networks: KAD, BitTorrent and I2P.

Several large scale P2P networks operating on the Internet are based on a Distributed Hash Table. These networks offer valuable services, but they all suffer from a critical issue allowing malicious nodes to be inserted in specific places on the DHT for undesirable purposes (monitoring, distributed denial of service, pollution, etc.). While several attacks and attack scenarios have been documented, few studies have measured the actual deployment of such attacks and none of the documented countermeasures have been tested for compatibility with an already deployed network. In our work, we focus on the KAD network. Based on large scale monitoring campaigns, we demonstrated that the world-wide deployed KAD network suffers large number of suspicious insertions around shared contents and we quantify them. To cope with these peers, we proposed a new efficient protection algorithm based on analyzing the distribution of the peers ID found

around an entry after a DHT lookup [3]. The evaluation of our solution showed that it detects the most efficient configurations of inserted peers with a very small false-negative rate, and that the countermeasures successfully filter almost all the suspicious peers. We demonstrate the direct applicability of our approach by implementing and testing our solution in real P2P networks

BitTorrent is a fast, popular, P2P filesharing application focused on fast propagation of content. Its trackerless approach uses a DHT based on Kademlia to search for sources when the hash of the metadata of the content to transfer is known. On the other hand, the eMule network uses the old ED2K protocol for filesharing including a system of priorized queues, but indexation is done through a solid Kademlia based DHT, named Kad. The Kad DHT stands for a search engine, wich provides an extra level to map keywords to file identifiers. We have designed an hybrid approach, compatible with both P2P file-sharing networks, which has the Kad advantages on indexation and the BitTorrent throughput for transfer while maintaining backward compatibility with both of these networks [42]. To validate our proposal we developed a prototype which supports content indexation provided by the Kad network and is able to transfer files using the BitTorrent protocol. Using this prototype, we measured the propagation of new content in clusters of aMule clients, BitTorrent clients, hybrid clients, and a mix of them.

In parallel, we continued our research about being anonymous when downloading from BitTorrent. Anonymous communications have been gaining more and more interest from Internet users as privacy and anonymity problems have emerged. Among anonymous enabled services, anonymous file-sharing is one of the most active one and is increasingly growing. Large scale monitoring on these systems allows us to grasp how they behave, which type of data is shared among users, the overall behavior in the system.

We presented the first monitoring study aiming to characterize the usage of the I2P network, a low-latency anonymous network based on garlic routing [23]. We characterized the file-sharing environment within I2P, and evaluated if this monitoring affects the anonymity provided by the network. We showed that most activities within the network are file-sharing oriented, along with anonymous web-hosting. We assessed the wide geographical location of nodes and network popularity. We also demonstrated that group-based profiling is feasible on this particular network [22].

Dedicated anonymous networks such as Freenet and I2P allow anonymous file-sharing among users. However, one major problem with anonymous file-sharing networks is that the available content is highly reduced, mostly with outdated files, and non-anonymous networks, such as the BitTorrent network, are still the major source of content. We showed that in a 30-days period, 21648 new torrents were introduced in the BitTorrent community, whilst only 236 were introduced in the anonymous I2P network, for four different categories of content. Therefore, how can a user of these anonymous networks access this varied and non-anonymous content without compromising its anonymity? In [24], we improved content availability in an anonymous environment by proposing the first internetwork model allowing anonymous users to access and share content in large public communities while remaining anonymous. We showed that our approach can efficiently interconnect I2P users and public BitTorrent swarms without affecting their anonymity nor their performance. Our model is fully implemented and freely usable.

6.4. Configuration security automation

Participants: Rémi Badonnel [contact], Martin Barrere, Olivier Festor.

The main research challenge addressed in this work is focused on enabling configuration security automation in autonomic networks and services. In particular our objective is to increase vulnerability awareness in the autonomic management plane in order to prevent configuration vulnerabilities. The continuous growth of networking significantly increases the complexity of management. It requires autonomic networks and services that are capable of taking in charge their own management by optimizing their parameters, adapting their configurations and ensuring their protection against security attacks. However, the operations and changes executed during these self-management activities may generate vulnerable configurations. A first part of our work in the year 2012 has been dedicated to the assessment of distributed vulnerabilities and to the elaboration of a collaborative management strategy for supporting their remediation. A configuration vulnerability is not

necessarily local but can also be spread over several devices in the autonomic network. We have showed in [8] how such distributed vulnerabilities can be mathematically formalized and described in a machine readable manner, through the specification of the DOVAL (Distributed OVAL) language on top of OVAL (Open Vulnerability and Assessment Language). We have designed and evaluated a dedicated framework for exploiting these vulnerability descriptions, collecting device configurations and detecting distributed vulnerabilities using specific aggregation techniques. Once a vulnerability is identified in the autonomic network, several remediation actions can potentially be performed by the autonomic network over devices. For that purpose, we have introduced an XCCDF-based specification for expressing alternative treatments related to a distributed vulnerability. We have also proposed a collaborative scheme for selecting one of these treatments depending on the current context (device capabilities and willingness to participate) [6]. A second part of our work has focused on the extension of our solution to other environments. In particular we have worked on the integration of our vulnerability assessment strategy over the Android plateform [9]. We have put forward a mathematical model as well as an optimized method that provides solid foundations for this context. By maintaining low-consumption services monitoring the system, the proposed approach minimizes heavy task executions by only triggering assessment activities when configuration changes are detected or new vulnerability definitions are available. In light of this, we have developed a prototype that efficiently performs self-assessment activities, and also introduces dedicated web services for collecting OVAL descriptions and storing assessment results. We have performed an analytical evaluation of the proposed model as well as an extensive set of technical experiments that shows the feasibility of our solution. We are currently working on the issue of past hidden vulnerable states. A network compromised in the past by an unknown vulnerability at that moment may still constitute a potential security threat in the present. Accordingly, past unknown system exposures are required to be taken into account. We are therefore investigating a novel strategy for identifying also such past hidden vulnerable configurations and increasing the overall security [9].

6.5. Cache Management in CCN

Participants: Thomas Silverston [contact], César Bernardini, Olivier Festor.

The Internet is currently mostly used for accessing content. Indeed, ranging from P2P file sharing to current video streaming services such as Youtube, it is expected that content will count for approximately 86% of the global consumer traffic by 2016.

While the Internet was designed for -and still focuses on- host-to-host communication (IP), users are only interested in actual content rather than source location. Hence, new Information-Centric Networking architectures (ICN) such as CCN, NetInf, Pursuit have been proposed giving high priority to efficient content distribution at large scale. Among all these new architectures, Content Centric Networking (CCN) has attracted considerable attention from the research community [2].

CCN is a network architecture based on named data where a packet address names content, not location. The notion of host as defined into IP does not exist anymore. In CCN, the content is not retrieved from a dedicated server, as it is the case for the current Internet. The premise is that content delivery can be enhanced by including per-node-caching as content traverses the network. Content is therefore replicated and located at different points of the network, increasing availability for incoming requests.

As content is cached along the path, it is crucial to investigate the caching strategy for CCN Networks and to propose new schemes adapted to CCN. We therefore designed *Most Popular Content* (MPC), a new caching strategy for CCN network [10].

Instead of storing all the content at every nodes on the path, MPC strategy caches only popular content. With MPC, each nodes count all the requests for a content and when it has been requested a large amount of time, the content will be cached at each node along the path. Otherwise, the content is not popular; it is transmitted but it is not cached into the network.

We implemented MPC into the ccnSim simulator and evaluate it through extensive simulations.

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

Our results demonstrate that using MPC strategy allow to achieve a higher Cache Hit in CCN networks and still reduces drastically the number of replicas. By caching only popular content, MPC helps at reducing the cache load at each node and the network resource consumption.

We expect that our strategy could serve as a base for studying name-based routing protocols. Being a suggestion based mechanism, it is feasible to adapt it to manage content among nodes, to predict popularity and to route content to destination. In addition, we are currently investigating the social relationship between users to improve our caching strategy for CCN networks.

6.6. QoS in Wireless Sensor Networks

Participants: François Despaux, Abdelkader Lahmadi, Bilel Nefzi, Hugo Cruz-Sanchez, Ye-Qiong Song [contact].

WSN research focus has progressively been moved from the energy issue to the QoS issue. Typical example is the MAC protocol design, which cares about not only low duty-cycle, but also high throughput with self-adaptation to dynamic traffic changes [21]. Our research on WSN QoS is thoroughly organized in three topics:

- MAC protocol design for both QoS and energy efficiency

  The main result that we obtained in 2012 is a new hybrid CSMA/TDMA MAC protocol, called Queue-MAC, that dynamically adapts the duty-cycle according to the current network traffic. The queue length of nodes is used as the network traffic indicator. When the traffic increases, the active CSMA period is accordingly extended by adding dynamic TDMA slots, allowing thus to efficiently handle burst traffic under QoS constraints. This protocol is implemented on the STM32W108 SOC chips and compared with both a fixed duty-cycle reference protocol and an optimized IEEE802.15.4 MAC protocol. Through extensive experimental measurements, we showed that our queue-length aware hybrid CSMA/TDMA MAC protocol largely outperforms the compared protocols. The proposed protocol can be easily implemented through slight adaptation of the IEEE802.15.4 standard [25].

  Many industrial WSN are based on IEEE802.15.4 standard. One of the critical issues is the scheduling of neighboring coordinators beacons. In [20], we presented TBoPS, a novel technique for scheduling beacons in the cluster-tree topology. TBoPS uses a dedicated period called beacon only period (BOP) to schedule beacons at the beginning of IEEE 802.15.4 superframe. The advantage of TBoPS is that every beacon-enabled node distributively selects a beacon schedule during association phase.

- QoS routing

  For supporting different QoS requirements, routing in WSN must simultaneously consider several criteria (e.g., minimizing energy consumption, hop counts or delay, packet loss probability, etc.). When multiple routing metrics are considered, the problem becomes a multi-constrained optimal path problem (MCOP), which is known as NP-complete. In practice, the complexity of the existing routing algorithms is too high to be implemented on the low cost and power constrained sensor nodes. Recently, Operator calculus (OC) has been developed by Schott and Staples with whom we collaborate. OC can be applied to solving MCOP problem with much lower complexity and can deal with dynamic topology changes (which is the case in duty-cycled WSN). The OC approach has been successfully applied to a concrete routing problem [13]. Its implementation over Contiki on TelosB motes has also been achieved, confirming thus its great potential for developing new QoS routing protocols for WSN.

- End-to-end performance in multi-hop networks

  Probabilistic end-to-end performance guarantee may be required when dealing with real-time applications. For instance, in our ANR QUASIMODO project, we considered an intrusion detection and tracking scenario and analyzed the application requirements with respect to the network QoS. Assuming the use of the extended Kalman filter based tracking technique, we derived the tradeoff

relationship between the tracking precision and the delay (from the target position and speed sampling to mobile nodes moving to cover the estimated next step area). In [5] we proposed a novel coordinative moving algorithm for autonomous mobile sensor networks to guarantee that the target can be detected in each observed step while minimizing the amount of moving sensors (so saving energy). In such kind of application context, we aim to provide methods for both network resource allocation and estimating the end-to-end delay in multi-hop WSN. Assuming IEEE802.15.4 WSN with cluster-tree routing, in [16] we addressed the problem of allocating and reconfiguring the available bandwidth using an Admission Control Manager that guarantees that the nodes respect their probabilistic bandwidth assignment when generating data traffic. It has been shown by simulation that using the proposed method, one can obtain desired probabilistic guarantee in both bandwidth and energy efficiency.

In a more general context of meshed networks, we present an empirical support of an analytical approach, which employs a frequency domain analysis for estimating end-to-end delay in multi-hop networks. The proposed analytical results of the end-to-end delay distribution are validated through simulation and compared with queuing theory based analysis. Our results demonstrate that an analytical prediction schema is insufficient to provide an adequate estimation of the end-to-end delay distribution function, but it requires to be combined with simulation methods for detailed link and node latency distribution [15].

6.7. Energy in Wireless Sensor Networks

Participants: Emmanuel Nataf [contact], Patrick-Olivier Kamgueu.

The energy sources of sensors in a wireless network rely mainly on batteries and are very limited in their capacity. Several research efforts are focalized on trying to limit the energy consumption in such networks. This is particularly the case in protocol design. Indeed, the communication consumes a large majority of the available energy. To be realistic and efficient, all proposed approaches need to know the energy available at any time in the systems. Unfortunately, most sensors do not provide such information because it requires additional built-in hardware that would drastically increase their cost. Over the last decade very accurate physical battery models that encompass consumption and recovery have been designed. The complexity of these models is however too high to be implemented inside simple sensors. Recent research results have shown that this integration could be possible if some approximations are integrated in the models.

We have worked on integrating such an approcimated model in the sensor operating system. This work allows the simulation of such sensors and the deployement on real devices that will be aware of their remaining energy level without requiring any additionnal costly equipment. A first implementation on simulation tool has given very promising results; sensors can access their energy level and take decision based on this estimate. Firstly, we have studied energy consumption of a sensors network collecting and routing data toward a single destination. Energy cost of the network deployment has been computed and so the network life as a whole. An other result of our work is the comparison of several common link layer access protocols and several data rate transmits [31].

6.8. Online Risk Management

Participants: Rémi Badonnel [contact], Oussema Dabbebi, Olivier Festor.

Telephony over IP has known a large scale deployment and has been supported by the standardization of dedicated signaling protocols. This service is however exposed to multiple attacks due to a lower confinement in comparison to traditional PSTN networks. While a large variety of methods and techniques has been proposed for protecting VoIP networks, their activation may seriously impact on the quality of such a critical service. Risk management provides new opportunities for addressing this challenge. In particular our work aims at performing online risk management for VoIP networks and services. The objective is to dynamically adapt the service exposure with respect to the threat potentiality, while maintaining a low security overhead. In the year 2012, we have pursued our work on online risk management and applied it to more distributed

configurations. In that context we have defined in [14] an exposure control solution for P2PSIP networks where the registration and location servers are implemented by a distributed hash table. After having analyzed different attack scenarios, we have designed the underlying risk management architecture and modelled several dedicated countermeasures. We have evaluated the performance and scalability of our approach through extensive experiments performed with the OMNET++ simulator. We have also proposed a trust-based solution for addressing residual attacks in the RELOAD framework. This latter, complementary to our risk management approach, is a peer-to-peer signalling overlay using a central certificate enrolment server and supporting P2PSIP infrastructures. Self-signed certificates can also be used in closed networks, and connections amongst nodes can be secured using an encryption protocol such as TLS. While the RELOAD framework permits to reduce the exposure to threats, P2PSIP networks are still exposed to residual attacks related to the routing and storage activities. For instance, it is trivial for a malicious node to refuse to give the stored information, or to send false routing messages in the network. We have showed how trust mechanisms can be exploited to counter these attacks in an efficient manner. Our work on online risk management has also focused on VoIP services in the Cloud [30]. The integration of IP telephony in this environment permits the delivery and access of new resources and constitutes an important factor for its scalability. While the Cloud has recently served as a basis for security attacks targeting IP telephony, such as SIP brute force attacks from the Amazon EC2 Cloud infrastructure, we consider that it also provides new possibilities for supporting the security of this service. We have analyzed the applicability of our online risk management approach in the Cloud, and evaluated to what extent security countermeasures may be outsourced as a service. We have mathematically defined a dedicated modelling and detailed different treatment strategies for applying countermeasures in the Cloud. Finally, we have quantified the benefits and costs of these strategies based on a set of experimental results.

6.9. Pervasive Computing

Participants: Laurent Ciarletta [contact], Olivier Festor, Ye-Qiong Song, Adrien Guenard, Yannick Presse.

Vincent Chevrier(MAIA Team), Thomas Navarrette Gutierrez (MAIA Team) and Priyadrsi Nanda (Universit of Technology, Sydney) did contribute to part of this activity.

In Pervasive or Ubiquitous Computing, a growing number of communicating/computing devices are collaborating to provide users with enhanced and ubiquitous services in a seamless way. In a related field, Cyber Physical Systems also are technological systems that have to be considered within a physical world and its contraints. They are complex systems where several inter-related phenomena have to be considered. In order to be studied, modeled and evaluated, we propose the use of co-simulation and multimodeling. to be Madynes is focusing on the networking aspects of such systems. We cooperate with toher the Maia team to be able to encompass issues and research questions that combine both networking and cognitive aspects.

Pervasive Computing is about interconnected and situated computing resources providing us(ers) with contextual services. These systems, embedded in the fabric of our daily lives, are complex: numerous interconnected and heterogeneous entities are exhibiting a global behavior impossible to forecast by merely observing individual properties. Firstly, users physical interactions and behaviors have to be considered. They are influenced and influence the environment. Secondly, the potential multiplicity and heterogeneity of devices, services, communication protocols, and the constant mobility and reorganization also need to be addressed. Our research on this field is going towards both closing the loop between humans and systems, physical and computing systems, and taming the complexity, using multi-modeling (to combine the best of each domain specific model) and co-simulation (to design, develop and evaluate) as part of a global conceptual and practical toolbox. We apply this work on UAvs and energy-constrained / location aware services.

In 2012 we worked on the following research topics :

- Continuing the work on multi-modeling and co-simulation, we've participated with the MAIA team on the development of an architecture for the control of complex systems based on multi-agent simulation [32], [2], and a CPS co-simulation (next item), and continue working on the AA4MM framework (Agents and artefacts for Multiple heterogeneous Models).

- In Cyper Physical Systems, we have lead the design and implementation of the Aetournos (Airborne Embedded auTonomOUs Robust Network of Objects and Sensors) platform at Loria. The idea of AETOURNOS is to build a platform which can be at the same time a demonstrator of scientific realizations and an evaluation environment for research works of various teams of our laboratory. It is also its own research domain : building a completely autonomous and robust flock of collaborating UAVs.

  In Madynes, we focus on the CPS and their networks and applications. Those systems consist of numerous autonomous elements in sharp interaction which functioning require a tight coupling between software implementations and technical devices. The collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of such a system. Indeed, if we look at the level of each of the elements playing a role into this system, a certain number of challenges and scientific questions can be studied: respect of real-time constraints of calculations for every autonomous UAV and for the communication between the robots, conception of individual, embedded, distributed or global management systems, development of self-adaptative mechanisms, conception of algorithms of collective movement etc... Furthermore, the answers to each of these questions have to finally contribute to the global functioning of the system. Applying co-simulation technique we plan to develop a hybrid "network-aware flocking behavior" / "behavior aware routing protocol". The platform is composed of several high-grade research UAVs (Pelican quadcopters and Firefly hexacopters) and lighter models (AR.Drone quacopters). We have provided a working set of tools : multi-simulation behavior / network / physics and generic software development using ROS (Robot Operating System). The UAVs carry a set of sensor for location awareness, their own computing capabilities and several wireless networks.

  This work is discribed in a position paper where a first implementation of a formation flight is detailed ([11]).
- Energy-constraint geolocalization, addressing, routing and management of wireless devices: a research collaboration with Fireflies RTLS was started in March 2009 and has ended in 2012. The initial work has been extended in a joint work with the former TRIO Team and a visiting professor from the University of Technology of Sydney. Its focus has been shiffted towards novel adressing and routing scheme minimizing a global energy-cost function in a wireless sensor network location systems [28]. We are proposing a global configuration tool for this matter in regards with given constraints (number of nodes, topology, QoS).

In 2013, we will continue working on the hybrid protocols and on the UAV platform, and apply our co-simulation work to Smart Grids.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

As part of our effort in Pervasive Computing research, we worked with Firelies RTLS, a French startup specialized in advanced geolocation services. The contract led to new routing schemes, QoS mand management protocols for Wireless Sensor Networks.

7.2. Bilateral Grants with Industry

We are active in the Alcatel Lucent/Bellabs Inria joint lab. This joint lab brings together research teams from Inria and Alcatel Lucent Bell Labs for addressing the key challenges of autonomous networking in three critical areas: semantic networking, high manageability and self-organized networks. Our activity is part of the joint initiative dedicated to high manageability, and focuses on security management aspects with the Alcatel-Lucent Bell Labs teams on network security. Our work in this joint lab concerns the automation of security management. It includes a first activity related to fuzzing, which includes the improvement of the

KiF framework as well as the design of novel fuzzing models for Alcatel-Lucent specific protocols. A second activity of the joint lab aims at investigating to what extent risk management strategies can be applied to VoIP infrastructures. The objective is to design and experiment dynamic risk management methods and techniques for voice oriented critical services.

8. Partnerships and Cooperations

8.1. Regional Initiatives

In 2012, the team was involved in the following initiative:

- CPER-SSS: in this initiative, the team did work on Scada networks security and P2P monitoring.

8.2. National Initiatives

8.2.1. ANR

The team did coordinate the VAMPIRE ANR Project which ended in october 2012. VAMPIRE is a research project funded by the French Research Agency (ANR, VERSO ANR-08-VERS-017) coordinated by the team. The goal of the project to investigate new thread security issues induced by Voice Over IP (VoIP) protocols and web2.0. Madynes has the lead on this project.

8.2.2. Actions d'Envergure Nationale

The Inria Large-scale initiative action AEN PAL project (http://pal.inria.fr) aims at providing technologies and services for improving the autonomy and quality of life for elderly and fragile persons. Communication is one of the key components for ensuring real-time data gathering and exchange between heterogeneous sensors and actuators (robots). Within PAL and thanks to the associated ADT PERCEE project, we extended MPIGate (http://mpigate.loria.fr), a multi-protocol interface and gateway, by integrating a publisher-subscriber data distribution model of standard middleware (DDS and ROS). The first experimentations showed its good performance and its easy-to-use interface for transparent heterogenous data access (through either programmer API or end-user web interface) [12]. The development and tests are conducted using LORIA's smart apartment platform developed within CPER MISN Informatique située project (http://infositu.loria.fr). The adoption of ROS (Robotic Operating System) also facilitates the interoperability of our services with the services of the other PAL partners since the new PALGate is based on ROS.

8.3. European Initiatives

8.3.1. FP7 Projects

8.3.1.1. Univerself

Title: Univerself

Type: COOPERATION (ICT)

Defi: The Network of the Future

Instrument: Integrated Project (IP)

Duration: September 2010 - August 2013

Coordinator: Alcatel Lucent (France)

Others partners:

Universiteit Twente,

Alcatel Lucent Ireland,

Alcatel Lucent Deutschland,

Valtion Teknillinen Tutkimuskeskus (Finland),

University of Piraeus,

France Telecom,

Telecom Italia,

National University of Athens,

Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung,

Interdisciplinary Institute for Broadband Technology,

Telefonica Investigacion y Desarrollo,

Thales Communications,

Inria,

Nec Europe,

University of Surrey,

University College London

IBBT (Belgium).

See also: http://www.univerself-project.eu/

Abstract: UniverSelf unites 17 partners with the aim of overcoming the growing management complexity of future networking systems, and to reduce the barriers that complexity and ossification pose to further growth. Univerself has been launched in October 2010 and is scheduled for four years.

8.3.1.2. FI-WARE

Type: COOPERATION (ICT)

Defi: PPP FI: Technology Foundation: Future Internet Core Platform

Instrument: Integrated Project (IP)

Duration: September 2011 - May 2014

Coordinator: Telefonica (Spain)

Others partners:Thales, SAP, Inria

See also: http://www.fi-ware.eu

Abstract: FI-WARE will deliver a novel service infrastructure, building upon elements (called Generic Enablers) which offer reusable and commonly shared functions making it easier to develop Future Internet Applications in multiple sectors. This infrastructure will bring significant and quantifiable improvements in the performance, reliability and production costs linked to Internet Applications ? building a true foundation for the Future Internet.

The key deliverables of FI-WARE will be an open architecture and a reference implementation of a novel service infrastructure, building upon generic and reusable building blocks developed in earlier research projects. We will demonstrate how this infrastructure supports emerging Future Internet (FI) services in multiple Usage Areas, and will exhibit significant and quantifiable improvements in the productivity, reliability and cost of service development and delivery, building a true foundation for the Future Internet.

The MADYNES contributions to the FI-WARE project are:

- Sicslowfuzzer, a fuzzing framework for the Internet of Things, that allows to assess the robustness of IoT OSes and applications, networkwise. More specifically, the tool uses the Scapy library for packet manipulation, allows users to define interaction scenarios in XML and provides multiple mutation algorithms;
- Flowoid, a netflow probe for Android-based devices, which also provides a netflow location template to convey location information of the device;
- XOvaldi4Android, an OVAL interpreter for Android-based devices, that is able to retrieve OVAL definitions using a web service, use them to check the current status of the system, and publish a result, using a second web service;
- coordination between the Security Work Package and the Inria teams involved in it. This included attending to weekly audio conferences, face to face meetings, and making sure deliverables and tasks were addressed in a timely manner.

8.3.2. Collaborations with Major European Organizations

Partner 1: Univeristy of Luxembourg (Luxembourg)

We have two ongoing PhD candidates with the SnT at Univeristy of Luxembourg. We do collaborate on Large Scale Monitoring for Security Management. Target services are: P2P Networks, Virtual Coordinates Systems and DNS Services.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Maroua BOUMESSOUER (from Mar 2012 until Aug 2012)

Subject: Etude des vulnérabilités et des attaques dans le protocole de routage RPL

Institution: Sup'Com Tunis (Tunisia)

Ayoub SOURY (from Mar 2012 until Aug 2012)

Subject: Vulnerabilities Prevention in Industrial Control Systems

Institution: Ecole Nationale des Sciences de l'Informatique (Tunisia)

Bernardo LAMAS (from Mar 2012 until Aug 2012)

Subject: Offensive Security for Industrial Control Systems

Institution: National University of Rosario (Argentina)

Tarang CHUGH (from Mar 2012 until Aug 2012)

Subject: Fairness Incentives for Multi-Protocol Cooperation in P2P Networks

Institution: Indraprastha Institute of Information Technology (India)

9. Dissemination

9.1. Scientific Animation

Olivier Festor is the Co-Chair together with Aiko Pras from University of Twente of the IFIP Working-Group 6.6 on Network and systems management. This working group is actively involved the animation of most major conferences in this research area and organizes frequent meetings and workshops on the domain.

Olivier Festor is the Co-chair together with Lisandro Zambenedetti Grandvile from the Federal University of Rio Grande do Sul (UFRGS) of the Internet Research Task Force (IRTF) Network Management Research Group since march 2011. We organized a Flow management workshop at the Inria premises in Paris during IETF 83.

Olivier Festor served as a TPC Member of the following 2012 events: IEEE/IFIP Network Operations and Management Symposium (NOMS'2012); IFIP IEEE in conjunction with ACM CNSM'2012; ICCVE'2012; Globecom CSSM'2012; PST 2012, AFRICOMM 2012 and Policy 2012.

Olivier Festor was Student Travel Grants co-chair for the IEEE/IFIP Network Operations and Management Symposium (IEEE NOMS'2012).

Olivier Festor is member of the board of editors of the Springer Journal of Network and Systems Management. He is member of the editorial board of the IEEE Transactions on Network and Service Management.

Olivier Festor server as a TPC Co-chair of the IEEE International Conference on Communications (IEEE ICC), Communication and Information System Security Symposium 2012. He also serves as a TPC member of the 2012 ICC Communication Software Services and Multimedia Applications Symposium (CSSMA).

Olivier Festor is the Research Director of EIT ICT Labs.

Isabelle Chrisment the Co-Chair together with Ahmed Serhrouchni from Telecom ParisTech of the IFIP Task Force 6.5 on Secure Networking This Task Force provides a framework for the organization of activities within the scope of secure networking. It facilitates international cooperation activities and exchanges in this area.

Isabelle Chrisment served as a TPC member of : the 6th International IFIP Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS'2012); the 13th joint TC6 and TC11 International IFIP Conference on Communications and Multimedia Security (IFIP CMS'2012) ; the Communication and Information Systems Security Symposium in the IEEE International Conference on Communications (IEEE ICC'12); the 14th french-speaking workshop on Algorithms in Telecommunications (Algotel'2012).

Remi Badonnel served as a TPC member of : the IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS'2012, PhD Symposium); the IEEE International Conference on Communications (IEEE ICC'12, CISS); the IEEE/IFIP Network Operations and Management Symposium (IEEE/IFIP NOMS'2012); the IEEE/IFIP International Workshop on Management of the Future Internet (IEEE/IFIP MANFI'2012); the International Conference on Cloud Computing and Services Science (CLOSER'2012).

Remi Badonnel chaired sessions at the following conferences:

- the IEEE International Conference on Communications (IEEE ICC'12, CISS),
- the IEEE/IFIP Network Operations and Management Symposium (IEEE/IFIP NOMS'2012),
- the IEEE/IFIP International Workshop on Management of the Future Internet (IEEE/IFIP MANFI'2012),
- the IEEE/IFIP/In Assoc. with ACM SIGCOMM International Conference on Network and Service Management (IEEE/IFIP/In Assoc. with ACM SIGCOMM CNSM'2012).

Ye-Qiong Song served as a TPC Member of the following 2012 events: the 17th IEEE international conference on Emerging Technologies & Factory Automation (ETFA'2012) ; the 9th IEEE international conference on Embedded Software and Systems (ICESS 2012) ; the 9th IEEE international workshop on Factory Communication Systems (WFCS 2012) ; the 10th International Conference On Smart homes and health Telematics (ICOST 2012); Workshop on Assistance and Service robotics in a human environment at IROS 2012; the International Workshop on Cooperative Robots and Sensor Networks (RoboSense 2012) in conjunction with the 3rd International Conference on Ambient Systems, Networks and Technologies (ANT-2012) ; the IEEE International Conference on Internet of Things (iThings 2012) ; the 11th International Workshop on Real-Time Networks (RTN 2012).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

There is a high demand on networking courses in the various universities in which LORIA takes part. This puts high pressure on 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, bachelor, master, ESIAL/TELECOM Nancy and École des Mines de Nancy engineering schools. In this section, we only enumerate the courses that are directly related to our research activity.

Laurent Andrey is the Head of Department of the Charlemagne IUT specialization on multimedia networking.

André Schaff is the Director of the ESIAL/TELECOM Nancy Engineering School. Isabelle Chrisment is co-directing the school and is in charge of the students recruitement process. Remi Badonnel is heading the Telecommunications and Networks specialization of the 2nd and 3rd years at the ESIAL/TELECOM Nancy engineering school, and is also in charge of the 2nd year design and development projects at the same school. They teach the networking related courses in this cursus.

Laurent Ciarletta is heading the specialization Safe Systems Architecture of the Computer Science and IT department of the Ecole des Mines de Nancy ("Grande Ecole", Engineering School, Master degree level). He is most notably in charge of Advanced Networking, Middleware, Component-based software development, Pervasive Computing, Networking and Systems courses at the Ecole des Mines de Nancy. Notably, within the ARTEM alliance (ICN - Business School, Mines Nancy, Ecole d'Art / School of Art), he is a member of the Research Comitee, more specifically with the "Smart Working Spaces" research theme, and he is co-responsible for the "Businesses: the digital challenge *CORP 3.0, Entreprises : le défi numérique* and the *Imagineries and the Workspaces*, 2 classes within the ARTEM alliance (over 90 hours).

Team members are teaching the following courses:

Licence : Laurent Andrey, Introduction to networks, 56, niveau L1 (DUT), IUT nancy-Charlemagne, France

Licence : Laurent Andrey, Introduction to network services, 38, niveau L2 (DUT), IUT nancy-Charlemagne, France

Ecole Ingénieur : Rémi Badonnel, Networks and Services Management, 24, niveau M2 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Rémi Badonnel, Industrial Project, 25, niveau M2 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Rémi Badonnel, Networks and Systems, 32, niveau M1 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Rémi Badonnel, Advanced Courses on Networks and Systems, 34, niveau M1 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Rémi Badonnel, Algorithmics, Data Structures and Algebra, 32, niveau L3 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Rémi Badonnel, Design and Development Project, 16, niveau M1 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Rémi Badonnel, Initiation to Research Project, 18, niveau M1 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Rémi Badonnel, Object-Oriented Programming, 32, niveau L3 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Rémi Badonnel, XML Design and Development, 20, niveau L3 Ingénieur, TELECOM Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Networking and Information System, 5, niveau L3 Ingénieur, Mines Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Bootcamp (programming bootcamp), 16, niveau M1 Ingénieur, Mines Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Operating Systems, 16, niveau M1 Ingénieur, Mines Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Networking, 27, niveau M1 Ingénieur, Mines Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Advanced Networking and Ambiant Systems, 18, niveau M1 Ingénieur, Mines Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Embedded Systems, 14, niveau M1 Ingénieur, Mines Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Advanced Software Engineering, 18, niveau M1 Ingénieur, Mines Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Middleware, 6, niveau M2 Ingénieur, Mines Nancy, France

Ecole Ingénieur : Laurent Ciarletta, Android development, 12, niveau M1 and M2 Ingénieur, Collegium Ingenieur and Mines Nancy, France

Master : Isabelle Chrisment, Sécurité des Réseaux et des Services, 12hTD, niveau M2, université de Lorraine, France

Ecole Ingénieur : Isabelle Chrisment, Langage C et Shell, 42hTD, niveau L3 Ingénieur, Telecom Nancy

Ecole Ingénieur : Isabelle Chrisment, Réseaux et Systèmes, 60hTD, niveau M1 Ingénieur, Telecom Nancy

Ecole Ingénieur : Isabelle Chrisment, Réseaux et Systèmes AvancÃ©s, 30hTD, niveau M1 Ingénieur, Telecom Nancy

Ecole Ingénieur : Isabelle Chrisment, , Routage Internet, 50hTD, niveau M2 Ingénieur, Telecom Nancy

Master : Isabelle Chrisment, Sécurité des Réseaux et des Applications, 18hTD, niveau M2, université de Lorraine, France

Ecole Ingénieur : Olivier Festor, P2P Algorithms, Protocols and Applications, 12, niveau M2 Ingénieur, Telecom Nancy & ENSEM, France

Ecole Ingénieur : Olivier Festor, Voix sur IP, Protocols and Applications, 9, niveau M2 Ingénieur, Telecom Nancy, France

Ecole Ingénieur : Abdelkader Lahmadi, Elements of Distributed Computing: algorithms and systems, 12, niveau M2 Ingénieur, ENSEM, France

Ecole Ingénieur : Abdelkader Lahmadi, Internet Protocols and Applications, 15, niveau M2 Ingénieur, ENSEM, France

Ecole Ingénieur : Abdelkader Lahmadi, Wireless Sensor Network Programming, 12, niveau M2 Ingénieur, ENSEM, France

Ecole Ingénieur : Abdelkader Lahmadi, Operating Systems and C language programming, 30, niveau M1 Ingénieur, ENSEM & Ecole des Mines de Nancy, France

Ecole Ingénieur : Abdelkader Lahmadi, Real time systems: concepts and programming, 30, niveau M1 Ingénieur, ENSEM & Ecole des Mines de Nancy, France

Ecole Ingénieur : Abdelkader Lahmadi, Relational Database, 20, niveau M1 Ingénieur, ENSEM, France

Ecole Ingénieur : Abdelkader Lahmadi, Java Programming, 50, niveau L1 Ingénieur, ENSEM, France

Ecole Ingénieur : Abdelkader Lahmadi, Computer Architecture ,50, niveau L1 Ingénieur, ENSEM, France

Ecole Ingénieur : Abdelkader Lahmadi, Techniques and Tools for Programming, 50, niveau L1 Ingénieur, Telecom Nancy, France

Licence : Thomas Silverston, De la Puce á l'Internet, 60, niveau L1, université de Lorraine, France

Master : Thomas Silverston, Réseaux Avancés, 87, niveau M2, université de Lorraine, France

Master : Thomas Silverston, Introduction aux Réseaux, 26, niveau M2, université de Lorraine, France

Master : Thomas Silverston, Voix sur IP, Contenu Multimédia, 38, M2, université de Lorraine, France

Licence : Thomas Silverston, Introduction aux Réseaux, 8, L3, université de Lorraine, France

Master : Ye-Qiong Song, Performance evaluation, 20, niveau M2, Université de Lorraine, France

Ecole Ingénieur : Ye-Qiong Song, Networking, 40, niveau M2, ENSEM - Universitd´e Lorraine, France

Ecole Ingénieur : Ye-Qiong Song, Database, 10, niveau M1, ENSEM - Universitd´e Lorraine, France

Ecole Ingénieur : Ye-Qiong Song, Algorithmic and progamming (Java), 120, niveau L3, ENSEM - Université de Lorraine, France

9.2.2. Supervision

PhD : Sheila Becker, Conceptual Approaches for Securing Networks and Systems, University of Luxembourg and Université de Lorraine, 10/2012, Thomas Engel, Olivier Festor, Radu State.

PhD in progress : Oussema Dabebbi,Dynamic risk management in Voice over IP services,oct., 2009, Supervised by Remi Badonnel and Olivier Festor

PhD in progress : Martin Barrere, Cooperative Vulnerability Management ,oct., 2010, Supervised by Remi Badonnel and Olivier Festor

PhD in progress : Monitoring and Security in P2P file sharing networks. Juan Pablo Timpanaro, May 2010, Isabelle Chrisment

PhD in progress : César Bernardini, Réseau orienté-contenu basé sur les communautés d'utilisateurs, 01/11/2011, Olivier Festor et Thomas Silverston

PhD in progress : Patrick Olivier Kamgueu, Energy management in WSNs, juin, 2012, Supervised by Emmanuel Nataf and Olivier Festor in France, Thomas Djotio in Cameroun

PhD in progress : Jamila Ben Slimane, Joint allocation of time slot and frenquency channels in wireless sensor networks, oct., 2008, Supervised by Ye-Qiong Song and Mounir Frikha

PhD in progress : François Despaux, Delay evaluation in wireless sensor networks for providing QoS, November 2011, Supervised by Ye-Qiong Song and Abdelkader Lahmadi

PhD in progress : Kevin Roussel : Dynamic management of QoS and energy in heterogenous sensor and actuator networks for e-health applications, December 2012, Supervised by Ye-Qiong Song

9.2.3. Juries

Team members participated to the following Ph.D. defense committees :

- Rafik Makhloufi, Ph.D. in Computer Science from Université Technologique de Troyes. Title: *Vers une gestion adaptative des réseaux complexes: cas de la surveillance de données agrégées*, February 2012. (Olivier Festor)
- Fernando Menezes Matos, Ph.D. in Computer Science from University of Coimbra. Title: *QoS for Multi-Domain Services in Next Generation Networks*, June 2012. (Olivier Festor)
- Sivasothy Shanmugalingam, Ph.D. in Computer Science from Telecom et Management Sud Paris. Title: *Convergence of Web and Communication Services*, April 2012. (Olivier Festor)

- Sabina Akhtar, Ph.D. in Computer Science from from Université de Lorraine. Title: *Verification of Distributed Algorithms using PlusCal-2*, May 2012. (Isabelle Chrisment)
- Tomas Navarrete Gutierrez, Ph.D in computer Science from Université de Lorraine. Title: *Une architecture de contrôle de systèmes complexes basée sur la simulation multi-agent*, October 2012. (Laurent Ciarletta)
- Fernand Lone Sang, Ph.D. in Computer Science from Université de Toulouse. Title: *Protection des systèmes informatiques contre les attaques par entrées-sorties*, November 2012. (Olivier Festor)
- Damien Roth, Ph.D. in Computer Science from Université de Strasbourg. Title: *Gestion de la mobilité dans les réseaux de capteurs sans fil*, Novembre 2012. (Isabelle Chrisment)
- Raphael Fournier-S'niehotta, Ph.D. in Computer Science from Université Pierre et Marie Curie - Sorbonne Universités. Title: *Détection et analyse d'une thématique rare dans de grands ensembles de requêtes : l'activité pédophile dans le P2P.*, December 2012. (Olivier Festor)
- Hai Anh Tran, Ph.D. in Computer Science from Université Paris Est. Title: *QoE-based Content Distribution Network Architecture*, December 2012. (Olivier Festor)
- Hien Thi Thu Truong, Ph.D. in Computer Science from Université de Lorraine. Title: *Un modèle de collaboration basée sur les contrats et la confiance*, December 2012. (Isabelle Chrisment)
- Aruna Jamdagni In, Ph.D. in Computer Science from University of Technology, Sydney Australia. Title: *Payload-based Anomaly Detection in HTTP Traffic,*. (Isabelle Chrisment)

Team members participated to the following Habilitation Degree defense committees :

- Pascal Anelli, Habilitation Degree in Computer Science from Université de la Réunion. Title: *Des aléas de la communication: de la transmission au transport*, April 2012. (Olivier Festor)
- Frédéric Weis, Habilitation Degree in Computer Science from Université de Rennes 1. Title: *Exploitation d'approches système dans les réseaux sans fil*, June 2012. (Olivier Festor)
- Ludovic Apvrille , Habilitation Degree in Computer Science from Université de Nice-Sophia Antipolis. Title: *Model-Based Design of Complex Embedded Systems*, December 2012. (Olivier Festor)
- Eric Totel, Habilitation Degree in Computer Science from Université de Rennes 1. Title: *Techniques de Détection d'Erreur Appliquées à la Détection d Intrusion*, Novembre 2012. (Isabelle Chrisment)
- Laurent Toutain, Habilitation Degree in Computer Science from Université Européenne de Bretagne. Title: *Vers un Internet Polymorphe*, December 2012. (Olivier Festor)

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] S. BECKER. *Conceptual Approaches for Securing Networks and Systems*, Institut National Polytechnique de Lorraine - INPL, October 2012, http://tel.archives-ouvertes.fr/tel-00768801.

[2] T. NAVARRETE GUTIERREZ. *Une architecture de contrôle de systèmes complexes basée sur la simulation multi-agent.*, Université de Lorraine, October 2012, http://tel.archives-ouvertes.fr/tel-00758118.

Articles in International Peer-Reviewed Journals

[3] T. CHOLEZ, I. CHRISMENT, O. FESTOR, G. DOYEN. *Detection and mitigation of localized attacks in a widely deloyed P2P network*, in "Journal of Peer-to-Peer Networking and Applications", May 2012 [*DOI :* 10.1007/s12083-012-0137-7], http://hal.inria.fr/hal-00766764.

[4] A. LAHMADI, O. FESTOR. *A Framework for Automated Exploit Prevention from Known Vulnerabilities in Voice Over IP Services*, in "IEEE Transactions on Network and Service Management", June 2012, vol. 9, n^{o} 2, p. 114-127 [*DOI :* 10.1109/TNSM.2012.011812.110125], http://hal.inria.fr/hal-00746977.

International Conferences with Proceedings

[5] J. BAI, P. CHENG, J. CHEN, A. GUÉNARD, Y.-Q. SONG. *Target Tracking with Limited Sensing Range in Autonomous Mobile Sensor Networks*, in "IEEE workshop WiSARN, in conjunction with IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS2012)", Hangzhou, Chine, IEEE Xplore, May 2012, p. 329-334, http://hal.inria.fr/hal-00745238.

[6] M. BARRÈRE, R. BADONNEL, O. FESTOR. *Collaborative Remediation of Configuration Vulnerabilities in Autonomic Networks and Systems*, in "8th IEEE International Conference on Network and Service Management (CNSM'12)", Las Vegas, États-Unis, IEEE Xplore, October 2012, http://hal.inria.fr/hal-00747646.

[7] M. BARRÈRE, R. BADONNEL, O. FESTOR. *Ovalyzer: an OVAL to Cfengine Translator*, in "IEEE/IFIP Network Operations and Management Symposium (NOMS'12)", Maui, Hawaii, États-Unis, Ph.D. Student Demo Contest of the IFIP/IEEE Network Operations and Management Symposium (NOMS'12), April 2012, http://hal.inria.fr/hal-00747656.

[8] M. BARRÈRE, R. BADONNEL, O. FESTOR. *Towards the Assessment of Distributed Vulnerabilities in Autonomic Networks and Systems*, in "IEEE/IFIP Network Operations and Management Symposium (NOMS'12)", Maui, Hawaii, États-Unis, IEEE xplore, April 2012, p. 335 - 342 [*DOI :* 10.1109/NOMS.2012.6211916], http://hal.inria.fr/hal-00747634.

[9] M. BARRÈRE, G. HUREL, R. BADONNEL, O. FESTOR. *Increasing Android Security using a Lightweight OVAL-based Vulnerability Assessment Framework*, in "5th IEEE Symposium on Configuration Analytics and Automation (SafeConfig'12)", Baltimore, États-Unis, IEEE Xplore, October 2012, http://hal.inria.fr/hal-00747640.

[10] C. BERNARDINI, T. SILVERSTON, O. FESTOR. *Towards Popularity-Based Caching in Content Centric Networks*, in "RESCOM 2012", Les Vosges, France, June 2012, http://hal.inria.fr/hal-00747611.

[11] L. CIARLETTA, A. GUÉNARD. *The AETOURNOS project: Using a flock of UAVs as a Cyber Physical System and platform for application-driven research*, in "2nd International Workshop on Emerging Topics on Sensor Networks (EmSens 2012)", Niagara Falls, Canada, ELSEVIER, August 2012, vol. 10, p. 939-945, Projet plateforme LORIA, http://hal.inria.fr/hal-00764055.

[12] H. CRUZ-SANCHEZ, L. HAVET, M. CHEHAIDER, Y.-Q. SONG. *MPIGate: A Solution to use Heterogeneous Networks for Assisted Living Applications*, in "The 9th IEEE International Conference on Ubiquitous Intelligence and Computing (UIC 2012)", Fukuaka, Japon, IEEE Xplore, September 2012, p. 104-111, http://hal.inria.fr/hal-00745155.

[13] H. CRUZ-SANCHEZ, S. STAPLES, R. SCHOTT, Y.-Q. SONG. *Operator Calculus Approach to Minimal Paths: Precomputed routing in a Store and Forward Satellite Constellation*, in "IEEE Globecom2012", Anaheim, California, États-Unis, IEEE Xplore, December 2012, To appear, http://hal.inria.fr/hal-00745161.

[14] O. DABBEBI, R. BADONNEL, O. FESTOR. *Dynamic Exposure Control in P2PSIP Networks*, in "2012 IEEE Network Operations and Management Symposium", Maui, États-Unis, IEEE Publisher, April 2012, p. 261-268, Laboratoire Commun Inria - Alcatel Lucent Bell Labs, http://hal.inria.fr/hal-00747508.

[15] F. DESPAUX, Y.-Q. SONG, A. LAHMADI. *Combining Analytical and Simulation Approaches for Estimating End-to-End Delay in Multi-hop Wireless Networks*, in "IEEE workshop WiSARN, in conjunction with IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS2012)", Hangzhou, Chine, IEEE Xplore, May 2012, p. 317-322, http://hal.inria.fr/hal-00745243.

[16] D. KHAN, B. NEFZI, L. SANTINELLI, Y.-Q. SONG. *Probabilistic Bandwidth Assignment in Wireless Sensor Networks*, in "The 7th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2012)", Yellow Mountains, Chine, X. WANG, R. ZHENG, K. JING (editors), Lecture Notes in Computer Science, Springer, August 2012, vol. 7405, p. 631-647, http://hal.inria.fr/hal-00745184.

[17] A. LAHMADI, C. BERNARDINI, O. FESTOR. *A Testing Framework for Discovering Vulnerabilities in 6LoWPAN Networks*, in "IEEE workshop WiSARN, in conjunction with IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS2012)", Hangzhou, Chine, July 2012, http://hal.inria.fr/hal-00747010.

[18] A. LAHMADI, L. CIARLETTA, A. BOEGLIN, O. FESTOR. *Routing based Roles Assignment for Monitoring 6LowPAN Networks*, in "Third International Conference on Communications and Networking (ComNet)", Hammamet, Tunisie, March 2012 [*DOI :* 10.1109/COMNET.2012.6217745], http://hal.inria.fr/hal-00747002.

[19] S. MARCHAL, J. FRANÇOIS, C. WAGNER, R. STATE, A. DULAUNOY, E. THOMAS, O. FESTOR. *DNSSM: A Large Scale Passive DNS Security Monitoring Framework*, in "2012 IEEE Network Operations and Management Symposium (NOMS) - miniconference", Lahaina, États-Unis, IEEE, April 2012, p. 988 - 993 [*DOI :* 10.1109/NOMS.2012.6212019], http://hal.archives-ouvertes.fr/hal-00749243.

[20] B. NEFZI, D. KHAN, Y.-Q. SONG. *TBoPS: a Tree based distributed Beacon only Period Scheduling mechanism for IEEE 802.15.4*, in "IEEE workshop WiSARN, in conjunction with IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS2012)", Hangzhou, Chine, IEEE Xplore, May 2012, p. 341-346, http://hal.inria.fr/hal-00745229.

[21] Y.-Q. SONG. *Protocoles auto-adaptatifs énergie-trafic pour les réseaux de capteurs sans fil*, in "8èmes journées francophones Mobilité et Ubiquité (Ubimob 2012)", Anglet, France, PH.ROOSE, N. COUTURE (editors), Cépaduès Editions (ISBN: 978.2.36493.018.6), June 2012, http://hal.inria.fr/hal-00745167.

[22] J. P. TIMPANARO, I. CHRISMENT, O. FESTOR. *A Bird's Eye View on the I2P Anonymous File-sharing Environment*, in "The 6th International Conference on Network and System Security", Wu Yi Shan, Chine, November 2012, http://hal.inria.fr/hal-00744919.

[23] J. P. TIMPANARO, I. CHRISMENT, O. FESTOR. *I2P's Usage Characterization*, in "Traffic Monitoring and Analysis - TMA 2012 (short paper)", Vienne, Autriche, March 2012, http://hal.inria.fr/hal-00744902.

[24] J. P. TIMPANARO, I. CHRISMENT, O. FESTOR. *Improving Content Availability in the I2P Anonymous File-Sharing Environment*, in "The 4th International Symposium on Cyberspace Safety and Security", Melbourne, Australie, Springer, December 2012, vol. 4, p. 77-92 [*DOI :* 10.1007/978-3-642-35362-8], http://hal.inria.fr/hal-00744922.

[25] S. ZHUO, Y.-Q. SONG, Z. WANG, Z. WANG. *Queue-MAC: A queue-length aware hybrid CSMA/TDMA MAC protocol for providing dynamic adaptation to traffic and duty-cycle variation in wireless sensor networks*, in "9th IEEE International Workshop on Factory Communication Systems (WFCS2012)", Lemgo/Detmold, Allemagne, IEEE Xplore, May 2012, p. 105-114, http://hal.inria.fr/hal-00745175.

Research Reports

[26] M. BARRÈRE, R. BADONNEL, O. FESTOR. *Vulnerability Assessment in Autonomic Networks and Services: a Survey*, Inria, July 2012, 14, http://hal.inria.fr/hal-00747659.

[27] M. BARRÈRE, R. BADONNEL, O. FESTOR. *Vulnerability Management and Past Experience in Autonomic Networks and Services*, Inria, September 2012, 8, http://hal.inria.fr/hal-00747660.

[28] L. CIARLETTA, H. CRUZ-SANCHEZ, Y.-Q. SONG, P. NANDA. *Routing Scheme for a Wireless Sensor Network Real-Time Locating System*, Inria, December 2012, 6, http://hal.inria.fr/hal-00764931.

[29] O. DABBEBI, R. BADONNEL, O. FESTOR. *An Online Risk Management Strategy for VoIP Enterprise Infrastructures*, Inria, August 2012, 18, http://hal.inria.fr/hal-00747585.

[30] O. DABBEBI, R. BADONNEL, O. FESTOR. *VoIP Security in the Cloud*, Inria, September 2012, 8, http://hal.inria.fr/hal-00747577.

[31] E. NATAF, O. FESTOR. *Online Estimation of Battery Lifetime for Wireless Sensors Network*, Inria, September 2012, 15, http://hal.inria.fr/hal-00730521.

[32] T. NAVARRETE GUTIERREZ, J. SIEBERT, L. CIARLETTA, V. CHEVRIER. *Influence of space and time dimensions in multi-agent models of the free-riding collective phenomenon*, Inria, May 2012, 22, http://hal.inria.fr/hal-00700643.

[33] B. SAADALLAH, A. LAHMADI, O. FESTOR. *CCNx for Contiki: implementation details*, Inria, November 2012, n^{O} RT-0432, 52, http://hal.inria.fr/hal-00755482.

Other Publications

[34] M. BOUMESSOUER. *Etude des vulnérabilités et desattaques dans le protocole de routage RPL*, December 2012, http://hal.inria.fr/hal-00766768.

[35] C. DESTRÉ, R. BADONNEL, B. MARTIN, O. FESTOR. *Synthesis of Deployment Results (Deliverable 4.6, Univerself)*, October 2012, Project Deliverable, http://hal.inria.fr/hal-00747539.

[36] O. FESTOR, A. LAHMADI. *Information Elements for device location in IPFIX*, July 2012, IETF Internet-Draft, http://hal.inria.fr/hal-00747053.

[37] G. HUREL. *An OVAL-based Vulnerability Assessment Framework for the Android Platform*, Université de Strasbourg, Nancy, August 2012, http://hal.inria.fr/hal-00747396.

[38] A. MANZALINI, R. BADONNEL, O. FESTOR. *Synthesis of Use Case Requirements R2 (Deliverable 4.6, Univerself)*, April 2012, Project Deliverable, http://hal.inria.fr/hal-00747549.

[39] A. MANZALINI, A. BANTOUNA, R. BADONNEL, M. BARRÈRE, O. FESTOR, S. CLAYMAN, R. CLEGG, A. GALIS, G. STYLIANOS. *Controlling Network Stability and Performance (UC2 White Paper, Univerself)*, August 2012, White Paper, http://hal.inria.fr/hal-00747529.

[40] B. SAADALLAH, A. LAHMADI, O. FESTOR. *CCNx in Every Sensor*, September 2012, http://hal.inria.fr/hal-00747041.

[41] G. STYLIANOS, R. BADONNEL, B. MARTIN, O. FESTOR. *Adaptation of Learning and Operation Methods to Specific Needs of Future Networks and Services (Deliverable 3.7, Univerself)*, September 2012, Project Deliverable, http://hal.inria.fr/hal-00747559.

[42] A. VICINO. *Using Kad-BitTorrent Hybrid Clients to Share Contents*, University of Buenos Aires, Buenos Aires, October 2012, 79, http://hal.inria.fr/hal-00766772.