
Activity Report 2012

# Project-Team PLANETE

## Protocols and applications for the Internet

RESEARCH CENTERS
**Sophia Antipolis - Méditerranée**
**Grenoble - Rhône-Alpes**

THEME
**Networks and Telecommunications**

# Table of contents

## Project-Team PLANETE

**Keywords:** Network Protocols, Wireless Networks, Security, Privacy, Monitoring, Peer-to-peer

*Creation of the Project-Team:* December 01, 2000 .

# 1. Members

**Research Scientists**

Walid Dabbous [Team Leader, Senior Researcher, Inria, Sophia Antipolis - Méditerranée, HdR]
Claude Castelluccia [Senior Researcher, Inria, Grenoble - Rhône-Alpes, HdR]
Thierry Turletti [Senior Researcher, Inria, Sophia Antipolis - Méditerranée, HdR]
Chadi Barakat [Junior Researcher, Inria, Sophia Antipolis - Méditerranée, HdR]
Mohamed Ali Kaafar [Junior Researcher, Inria, Grenoble - Rhône-Alpes]
Cédric Lauradoux [Junior Researcher, Inria, Grenoble - Rhône-Alpes]
Daniel Le Métayer [Senior Researcher, Inria, Grenoble - Rhône-Alpes, HdR]
Arnaud Legout [Junior Researcher, Inria, Sophia Antipolis - Méditerranée]
Vincent Roca [Junior Researcher, Inria, Grenoble - Rhône-Alpes]

**Engineers**

Jonathan Detchart [Expert Engineer, Grenoble - Rhône-Alpes]
Thierry Parmentelat [Dream Engineer, Sophia Antipolis - Méditerranée]
Alina Quereilhac [Expert Engineer and PhD student, Sophia Antipolis - Méditerranée]
Fabrice Schuler [Expert Engineer, Grenoble - Rhône-Alpes]
Daniel Camara [Experienced Engineer, Sophia Antipolis - Méditerranée]
Fréderic Urbani [Expert Engineer, Sophia Antipolis - Méditerranée]
Julien Tribino [Associate Engineer, Sophia Antipolis - Méditerranée]
Mohamed Larabi [Expert Engineer since March 2012, Sophia Antipolis - Méditerranée]
Lucia Guevgeozian Odizzio [Expert Engineer since October 2012, Sophia Antipolis - Méditerranée]
Gergely Acs [Expert Engineer, since May 2012, Grenoble - Rhône-Alpes]

**PhD Students**

Sana Ben Hamida [Funding CEA LETI, Grenoble - Rhône-Alpes]
Abdelberi Chaabane [Funding ANR ARESA2 contract, Grenoble - Rhône-Alpes]
Ludovic Jacquin [Minalogic Inria grant, Grenoble - Rhône-Alpes]
Ferdaouss Mattoussi [Funding ADR Alcatel Lucent contract, Grenoble - Rhône-Alpes]
Ashwin Rao [Funding OneLab2 and Connect projects, Sophia Antipolis - Méditerranée]
Shafqat Ur-Rehman [Funding F-Lab project, until January 2012, Sophia Antipolis - Méditerranée]
Anshuman Kalla [Funding FRM, until June 2012, Sophia Antipolis - Méditerranée]
Xuan Nam Nguyen [Funding FRM, since October 2012, Sophia Antipolis - Méditerranée]
Dong Wang [Funding ANR PFlower project, Grenoble - Rhône-Alpes]
Minh-Dung Tran [Funding Allocation of Ministry of national Education, Grenoble - Rhône-Alpes]
Lukasz Olejnik [Funding Inria Cordi, Grenoble - Rhône-Alpes]
Maksym Gabielkov [Funding Allocation of Ministry of national Education, Sophia Antipolis - Méditerranée]
Wunan Gong [Funding OpenLab, since March 2012, Sophia Antipolis - Méditerranée]
Thibaud Antignac [Funding Inria CORDI-S scholarship, Grenoble - Rhône-Alpes]
Riccardo Ravaioli [Funding UCN@Sophia Laboratory of Excellence scholarship, Sophia Antipolis - Méditerranée]

**Post-Doctoral Fellows**

Young-Hwan Kim [Funding Inria CIRIC, Sophia Antipolis - Méditerranée]
Damien Saucez [Funding Inria scholarship, DPE, Sophia Antipolis - Méditerranée]
Byungchul Park [Funding Inria scholarship, DRI, Sophia Antipolis - Méditerranée]

Gergely Acs [Funding Inria, until April 2012, Grenoble - Rhône-Alpes]
Mathieu Cunche [Funding Inria-Schneider, from May 2012 to September 2012, Grenoble - Rhône-Alpes]
Daniele Perito [Funding Inria Relations Internationales, from December 2011 to October 2012, Grenoble - Rhône-Alpes]
Denis Butin [Funding FP7 FI-WARE project, since July 2011, Grenoble - Rhône-Alpes]

**Visiting Scientists**

Mostafa Ammar [Visiting Professor from Georgia Tech, June 2012, Sophia Antipolis - Méditerranée]
Paul de Hert [Visiting Professor from Free University of Brussels, June 2012, Grenoble - Rhône-Alpes]
Katia Obraczka [Visiting Professor from UCSC, June 2012, Sophia Antipolis - Méditerranée]
Marc Mendonca [Visiting PhD student from UCSC, from Sep 2012 until Dec 2012, Sophia Antipolis - Méditerranée]
Ilaria Cianci [Visiting PhD student from Politecnico di Bari, from November 2012 until August 2013, Sophia Antipolis - Méditerranée]

**Administrative Assistants**

Anais Cassino [Sophia, until May 2012, Sophia Antipolis - Méditerranée]
Christine Claux [Sophia, from June 2012, Sophia Antipolis - Méditerranée]
Helen Pouchot [Grenoble, Grenoble - Rhône-Alpes]

**Others**

Riccardo Ravaioli [Ubinet intern, from March to August 2012, Sophia Antipolis - Méditerranée]
Lucia Guevgeozian Odizzio [University of the Republic Uruguay intern, from May to September 2012, Sophia Antipolis - Méditerranée]
Xuan-Nam Nguyen [Ubinet intern, from March to August 2012, Sophia Antipolis - Méditerranée]
Maksym Gabielkov [Ubinet intern, from March to August 2012, Sophia Antipolis - Méditerranée]
Francisco Santos [EPFL intern, from February to August 2012, Sophia Antipolis - Méditerranée]
Tessema Mindaye [Ubinet intern, from March to August 2012, Sophia Antipolis - Méditerranée]
Sumit Bansal [IIT Ropal Intern, from February to July 2012, Grenoble - Rhône-Alpes]

# 2. Overall Objectives

## 2.1. Introduction

The Planète group, located both at Inria Sophia Antipolis - Méditerranée and Inria Grenoble - Rhône-Alpes research centers, conducts research in the domain of networking, with an emphasis on designing, implementing, and evaluating Internet protocols and applications. The main objective of the group is to propose and study new architectures, services and protocols that will enable efficient and secured communication through the Internet.

The Internet is a huge success: its scale has increased by several orders of magnitude. In order to cope with such growth, the simple, original Internet architecture has accreted several hundred additional protocols and extensions. Networks based upon this significantly more complex architecture are increasingly difficult to manage in a way that enables the qualities of service delivered to meet the needs of the over 1 billion users.

The increasing, and implicit, reliance on the Internet has stimulated a major debate amongst experts as to whether the current architecture and protocols can continue to be patched, or whether it will collapse under the demands of future applications. There are signs that the current suite of protocols and solutions are becoming inadequate to cope with some common Internet trends: mobility of users and devices, unusual but legitimate traffic load (e.g. flash crowds), large heterogeneity in terms of devices' capabilities and service features, delivery of real-time high-bandwidth video services, requirements for episodic connectivity, scalability in terms of number of nodes and users, complexity related to network, service and security management.

Additionally, the original Internet was designed and built in an era of mutual trust, probably due to the small size of the "ARPANet" research community. Many of the protocol additions/extensions have been to retrofit protection mechanisms that are required in the current Internet environment, which does not merit mutual trust. The volume and types of attempts to subvert the Internet will continue to increase, further stressing the current architecture. Current solutions for security are added a posteriori as a patch to overcome the limitations encountered, instead of being embedded in the system functionality.

Furthermore, mobile network hosts are rapidly becoming the norm for the devices with which users access the Internet. An increasing number of the protocol additions/extensions have been needed to retrofit support for mobility into the (initially wireline-focussed) Internet architecture. The growing use of mobile sensors will continue to drive the need for solid mobility support in the architecture (and the efficient transfer of small data units).

The Planète project-team addresses some of these problems related to both (global) architectural and (specific) protocol aspects of the future Internet. Our research directions span several areas such as data-centric architectures; network security; network monitoring and network evaluation platforms.

Our research activities are realized in the context of French, European and international collaborations: in particular with several academic (UCLA, Berkeley, UCSC, Princeton U., U. Washington, UC Irvine, NYU, NICTA, ICT-CAS (China), Concordia U., KTH, CASED, TUB, Cambridge, U. Bari, U. Diego Portales, U. Berne, EPFL, U. Pisa, RPI, ENSI (Tunis), LIP6, Eurecom, Univ. de Savoie, INSA Lyon, Ensimag, University de Rennes, etc.) and industrial (Ericsson, Nokia, SUN, Docomo, Expway, Alcatel, Orange R&D, Coronis, STMicroelectronics, Motorola, Technicolor, Netcelo, NEC, Boeing, etc.) partners.

## 2.2. Highlights of the Year

- Our paper entitled “I know who you will meet this evening! Linking wireless devices using Wi-Fi probe requests,” got the Best Paper Award – Runner Up, in IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2012), San Francisco, California, USA.
- After several years of heavy involvement in the IETF activities in the transport and routing areas, four document authored or co-authored by project-team members reached the RFC status in 2012.
  - RFC 6726 (“Standards Track”) is a revision of the RFC 3926 that specifies FLUTE, the application that enables the reliable transmission of multimedia files to a large set of receivers, typically portable devices (smartphones). Over the years FLUTE and the underlying transport protocol, ALC, became key components that are now part of all the wireless Internet standards. This revision benefits from the insight gained by the deployment and usage of these components since 2006.
  - RFC 6584 (“Standards Track”) explains how to use classic authentication and integrity schemes (i.e. group MAC and digital signatures) in the ALC and NORM reliable multicast protocols. All the applications built on top of them, FLUTE for instance, directly benefit from this service.
  - RFC 6816 (“Standards Track”) specifies how to use the LDPC-Staircase AL-FEC codes (that we previously specified in RFC 5170) in the context of FECFRAME, a framework that enables AL-FEC codes to be dynamically and flexibly inserted in communication stacks for improved robustness. The typical use-case is the reliable delivery of multimedia contents in streaming mode. Therefore this RFC 6816 enlarges the fields of application of our LDPC-Staircase codes, initially designed to address file delivery use-cases (e.g. with FLUTE/ALC), to the realtime transmission of contents in streaming mode.
  - RFC 6834 (“Experimental Track”) specifies a mechanism to enforce state consistency between LISP sites by using version numbers in LISP mappings. LISP (Locator/ID Separation Protocol) uses mappings and encapsulation to improve the scalability of Internet routing and data-centers. This RFC is an enabler for fast and scalable resiliency and mobility techniques in LISP but also for state consistency in complex LISP (e.g., large datacenters).

# 3. Scientific Foundations

## 3.1. Experimental approach to Networking

Based on a practical view, the Planète approach to address the above research topics is to design new communication protocols or mechanisms, to implement and to evaluate them either by simulation or by experimentation on real network platforms (such as PlanetLab and OneLab). Our work includes a substantial technological component since we implement our mechanisms in pre-operational systems and we also develop applications that integrate the designed mechanisms as experimentation and demonstration tools. We also work on the design and development of networking experimentation tools such as the ns-3 network simulator and experimental platforms. We work in close collaboration with research and development industrial teams.

In addition to our experimentation and deployment specificities, we closely work with researchers from various domains to broaden the range of techniques we can apply to networks. In particular, we apply techniques of the information and queuing theories to evaluate the performance of protocols and systems. The collaboration with physicists and mathematicians is, from our point of view, a promising approach to find solutions that will build the future of the Internet.

In order to carry out our approach as well as possible, it is important to attend and contribute to IETF (Internet Engineering Task Force) and other standardization bodies meetings on a regular basis, in order to propose and discuss our ideas in the working groups related to our topics of interests.

# 4. Application Domains

## 4.1. Next Generation Networks

The next-generation network must overcome the limitations of existing networks and allow adding new capabilities and services. Future networks should be available anytime and anywhere, be accessible from any communication device, require little or no management overhead, be resilient to failures, malicious attacks and natural disasters, and be trustworthy for all types of communication traffic. Studies should therefore address a balance of theoretical and experimental researchs that expand the understanding of large, complex, heterogeneous networks, design of access and core networks based on emerging wireless and optical technologies, and continue the evolution of Internet. On the other hand, it is also highly important to design a next-generation Internet which we will call the "Future Internet" from core functionalities in order to ensure security and robustness, manageability, utility and social need, new computing paradigms, integration of new network technologies and higher-level service architectures.

To meet emerging requirements for the Internet's technical architecture, the protocols and structures that guide its operation require coordinated, coherent redesign. A new approach will require rethinking of the network functions and addressing a range of challenges. These challenges include, but are not limited to, the following examples:

- New models for efficient data dissemination;
- Coping with intermittent connectivity;
- The design of secured, privacy protecting, and robust networked systems;
- Understanding the Internet behavior;
- Building network evaluation platforms.

The following research directions are essential building blocks we are contributing to the future Internet architecture.

### Towards Data-Centric Networking

From the Internet design, back to 1970, the resources to be addressed and localized are computers. Indeed, at that time there were few machines interconnected, and nobody believed this number would ever be larger than a few tens of thousand of machines. Moreover, those machines where static machines with well identified resources (e.g., a given hierarchy of files) that were explicitly requested by the users. Today, the legacy of this architecture is the notion of URLs that explicitly address specific resources on a specific machine. Even if modern architectures use caches to replicate contents with DNS redirection to make those caches transparent to the end-users, this solution is only an hack that do not solve today's real problem: Users are only interested in data and do not want anymore to explicitly address where those data are. Finding data should be a service offered by the network. In this context of data-centric network, which means that the network architecture is explicitly built to transparently support the notion of content, a data can be much more than a simple content. In such a network you can, of course, request a specific file without explicitly specifying its location, the network will transparently return the closest instance of the content. You can also request a specific service from a person without knowing its explicit network location. This is in particular the case of a VoIP or an instant messaging conversation. A data-centric architecture is much more than a simple modification of the naming scheme currently used in the Internet. It requires a major rethinking a many fundamental building blocks of the current Internet. Such networking architecture will however allow seamless handling of the tricky problematic of *episodic connectivity*. It also shifts the focus from transmitting data by geographic location, to *disseminating* it via named content. In the Planète project-team, we start to work on such data-centric architectures as a follow-up and federating axe for three of our current activities (adaptive multimedia transmission protocols for heterogeneous networks, data dissemination paradigms and peer-to-peer systems). It is important to study such data-centric architectures considering in particular the corresponding naming problem, routing and resource allocation, reliable transport, data security and authentication, content storage.

Today's Internet is characterized by high node and link heterogeneity. Nodes may vary substantially in terms of their processing, storage, communication, and energy capabilities. They may also exhibit very different mobility characteristics, from static nodes to nodes that are considerably mobile (e.g., vehicles). Links may be wired or wireless and thus operate at widely varying rates and exhibit quite different reliability characteristics. One of the challenges of data-centric architecture is to provide access to data anytime anywhere in the presence of high degree of heterogeneity. This means that the network will not be connected all the time, due to a number of factors such as node mobility, link instability, power-aware protocols that, for example, turn nodes off periodically, etc. Additionally, disconnections may last longer than what "traditional" routing protocols (e.g., MANET routing) can handle. These types of network, a.k.a, intermittently connected networks, or even episodically connected networks, have recently received considerable attention from the networking research community. Several new routing paradigms have been proposed to handle possibly frequent, long-lived disconnections. However, a number of challenges remain, including: (1) The support of scalable and transparent integration with "traditional" routing mechanisms including wired infrastructure, infrastructure-based wireless and MANET routing. (2) The study of heuristics for selecting forwarding nodes (e.g., based on node's characteristics such as node's speed, node's resources, sociability level, node's historic, etc. (3) The design of unicast and multicast transmission algorithms with congestion and error control algorithms tailored for episodically connected networks and taking into account the intrinsic characteristics of flows. (4) The design of incentive-based mechanisms to ensure that nodes forward packets while preventing or limiting the impact of possible misbehaving nodes. The solutions proposed, which are likely to extensively use cross-layer mechanisms, will be evaluated using the methodology and the tools elaborated in our new *Experimental Platform* research direction.

On the other hand, multicast/broadcast content delivery systems are playing an increasingly important role in data-centric networking. Indeed, this is an optimal dissemination technology, that enables the creation of new commercial services, like IPTV over the Internet, satellite-based digital radio and multimedia transmission to vehicles, electronic service guide (ESG) and multimedia content distribution on DVB-H/SH networks. This is also an efficient way to share information in WiFi, WiMax, sensor networks, or mobile ad hoc infrastructures. Our goal here is to take advantage of our strong background in the domain to design an *efficient, robust (in particular in case of tough environments) and secure (since we believe that security considerations will play an increasing importance) broadcasting system*. We address this problem by focusing on the following

activities: (1) The protocols and applications that enable the high level control of broadcasting sessions (like the FLUTE/ALC sessions) are currently missing. The goal is to enable the content provider to securely control the underlying broadcasting sessions, to be able to launch new sessions if need be, or prematurely stop an existing session and to have feedback and statistics on the past/current deliveries. (2) The AL-FEC building block remains the cornerstone on which the whole broadcasting system relies. The goal is to design and evaluate new codes, capable of producing a large amount of redundancy (thereby approaching rateless codes), over very large objects, while requiring a small amount of memory/processing in order to be used on lightweight embedded systems and terminals. (3) The security building blocks and protocols that aim at providing content level security, protocol level security, and network level security must be natively and seamlessly integrated. This is also true of the associated protocols that enable the initialization of the elementary building blocks (e.g. in order to exchange security parameters and keys). Many components already exist. The goal here is to identify them, know how to optimally use them, and to design/adapt the missing components, if any. (4) It is important seamlessly integrated these broadcasting systems to the Internet, so that users can benefit from the service, no matter where and how he is attached to the network. More precisely we will study the potential impacts of a merge of the broadcasting networks and the Internet, and how to address them. For instance there is a major discrepancy when considering flow control aspects, since broadcasting networks are using a constant bit rate approach while the Internet is congestion controlled.

When a native broadcasting service is not enabled by the network, data should still be able to be disseminated to a large population in a scalable way. A peer-to-peer architecture supports such an efficient data dissemination. We have gained a fundamental understanding of the key algorithms of BitTorrent on the Internet. We plan to continue this work in two directions. First, we want to study how a peer-to-peer architecture can be natively supported by the network. Indeed, the client-server architecture is not robust to increase in load. The consequence is that when a site becomes suddenly popular, it usually becomes unreachable. The peer-to-peer architecture is robust to increase in load. However, a native support in the network of this architecture is a hard problem as it has implications on many components of the network (naming, addressing, transport, localization, etc.). Second, we want to evaluate the impact of wireless and mobile infrastructures on peer-to-peer protocols. This work has started with the European project Expeshare. The wireless medium and the mobility of nodes completely change the properties of peer-to-peer protocols. The dynamics becomes even more complex as it is a function of the environment and of the relative position of peers.

## Network security and Privacy

The Internet was not designed to operate in a completely open and hostile environment. It was designed by researchers that trust each other and security at that time was not an issue. The situation is quite different today and the Internet community has drastically expanded. The Internet is now composed of more than 300 millions computers worldwide and the trust relationship has disappeared. One of the reason of the Internet success is that it provides ubiquitous inter-connectivity. This is also one of the its main weakness since it allows to launch attacks and to exploit vulnerabilities in a large-scale basis. The Internet is vulnerable to many different attacks, for example, Distributed Denial-of Service (DDoS) attacks, epidemic attacks (Virus/Worm), spam/phishing and intrusion attacks. The Internet is not only insecure but it also infringes users' privacy. Those breaches are due to the Internet protocols but also to new applications that are being deployed (VoIP, RFID,...). A lot of research is required to improve the Internet security and privacy. For example, more research work is required to understand, model, quantify and hopefully eliminate (or at least mitigate) existing attacks. Furthermore, more and more small devices (RFIDs or sensors) are being connected to the Internet. Current security/cryptographic solutions are too expensive and current trust models are not appropriate. New protocols and solutions are required : security and privacy must be considered in the Internet architecture as an essential component. The whole Internet architecture must be reconsidered with security and privacy in mind. Our current activities in this domain are on security in wireless, ad hoc and sensor networks, mainly the design of new key exchange protocols and of secured routing protocols. We also work on location privacy techniques, authentication cryptographic protocols and opportunistic encryption. We plan to continue our research on wireless security, and more specifically on WSN and RFID security focusing on the design of real and

deployable systems. We started a new research topic on the security of the Next-Generation Internet. The important goal of this new task is to rethink the architecture of the Internet with security as a major design requirement, instead of an after-thought.

**Wireless Sensor Networks**: A lot of work has been done in the area of WSN security in the last years, but we believe that this is still the beginning and a lot of research challenges need to be solved. On the one hand it is widely believed that the sensor networks carry a great promise: Ubiquitous sensor networks will allow us to interface the physical environment with communication networks and the information infrastructure, and the potential benefits of such interfaces to society are enormous, possibly comparable in scale to the benefits created by the Internet. On the other hand, as with the advent of the Internet, there is an important associated risk and concern: How to make sensor network applications resilient and survivable under hostile attacks? We believe that the unique technical constraints and application scenarios of sensor networks call for new security techniques and protocols that operate above the link level and provide security for the sensor network application as a whole. Although this represents a huge challenge, addressing it successfully will result in a very high pay-off, since targeted security mechanisms can make sensor network operation far more reliable and thus more useful. This is the crux of our work. Our goal here is to design new security protocols and algorithms for constrained devices and to theoretically prove their soundness and security. Furthermore, to complement the fundamental exploration of cryptographic and security mechanisms, we will simulate and evaluate these mechanisms experimentally.

**RFID**: As already mentioned, the ubiquitous use of RFID tags and the development of what has become termed "the Internet of things" will lead to a variety of security threats, many of which are quite unique to RFID deployment. Already industry, government, and citizens are aware of some of the successes and some of the limitations or threats of RFID tags, and there is a great need for researchers and technology developers to take up some of daunting challenges that threaten to undermine the commercial viability of RFID tags on the one hand, or to the rights and expectations of users on the other. We will focus here on two important issues in the use of RFID tags: (1) *Device Authentication*: allows us to answer several questions such as: Is the tag legitimate? Is the reader a tag interacts with legitimate? (2) *Privacy*: is the feature through which information pertaining to a tag's identity and behavior is protected from disclosure by unauthorized parties or by unauthorized means by legitimate parties such as readers. In a public library, for example, the information openly communicated by a tagged book could include its title or author. This may be unacceptable to some readers. Alternatively, RFID- protected pharmaceutical products might reveal a person's pathology. Turning to authenticity, if the RFID tag on a batch of medicines is not legitimate, then the drugs could be counterfeit and dangerous. Authentication and privacy are concepts that are relevant to both suppliers and consumers. Indeed, it is arguable that an RFID deployment can only be successful if all parties are satisfied that the integrity between seller and buyer respects the twin demands of authentication and privacy. Our main goal here, therefore, is to propose and to prototype the design of cryptographic algorithms and secure protocols for RFID deployment. These algorithms and protocols may be used individually or in combination, and we anticipate that they will aid in providing authentication or privacy. One particular feature of the research in the RFID-AP project is that the work must be practical. Many academic proposals can be deeply flawed in practice since too little attention has been paid to the realities of implementation and deployment. This activity will therefore be notable for the way theoretical work will be closely intertwined with the task of development and deployment. The challenges to be addressed in the project are considerable. In particular there are demanding physical limits that apply to the algorithms and protocols that can be implemented on the cheapest RFID tags. While there often exist contemporary security solutions to issues such as authentication and privacy, in an RFID-based deployment they are not technically viable. And while one could consider increasing the technical capability of an RFID-tag to achieve a better range of solutions, the solution is not economically viable.

**Next Generation Internet Security**: The current Internet has reached its limits; a number of research groups around the world are already working on future Internet architectures. The new Internet should have built-in security measures and support for wireless communication devices, among other things. A new network design is needed to overcome unwanted traffic, malware, viruses, identity theft and other threats plaguing today's Internet infrastructure and end hosts. This new design should also enforce a good balance between privacy and

accountability. Several proposals in the area have been made so far, and we expect many more to appear in the near future. Some mechanisms to mitigate the effects of security attacks exist today. However, they are far from perfect and it is a very open question how they will behave on the future Internet. Cyber criminals are very creative and new attacks (e.g. VoIP spam, SPIT) appear regularly. Furthermore, the expectation is that cyber criminals will move into new technologies as they appear, since they offer new attack opportunities, where existing countermeasures may be rendered useless. The ultimate goal of this research activity is to contribute to the work on new Internet architecture that is more resistant to today's and future security attacks. This goal is very challenging, since some of future attacks are unpredictable. We are analyzing some of the established and some of the new architectural proposals, attempting to identify architectural elements and patterns that repeat from one architectural approach to another, leading to understanding how they impact the unwanted traffic issue and other security issues. Some of the more prominent elements are rather easy to identify and understand, such as routing, forwarding, end-to-end security, etc. Others may well be much harder to identify, such as those related to data-oriented networking, e.g., caching. The motivation for this work is that the clean slate architectures provide a unique opportunity to provide built in security capabilities that would enable the prevention of phenomenon like unwanted traffic. New architectures will most likely introduce additional name-spaces for the different fundamental objects in the network and in particular for routing objects. These names will be the fundamental elements that will be used by the new routing architectures and security must be a key consideration when evaluating the features offered by these new name-spaces.

## Network Monitoring

The Planète project-team contributes to the area of network monitoring. Our focus is on the monitoring of the Internet for the purpose of access quality assessment, problem detection and troubleshooting. Indeed, in the absence of an advanced management and control plan in the Internet, and given the simplicity of the service provided by the core of the network and the increase in its heterogeneity, it is nowadays common that users experience a service degradation and are unable to understand the reasons for the access quality they perceive. Problems at the access can be in the form of a pure disconnection, a decrease in the bandwidth or an increase in the delay or loss rate of packets. Service degradation can be caused by protocol anomalies, an attack, an increase in the load, or simply a problem at the source or destination machines. Actually, it is not easy to diagnose the reasons for service degradation. Basic tools exist as ping and trace-route, but they are unable to provide detailed answers on the source of the problem nor on its location. From operator point of view, the situation is not better since an operator has only access to its own network and can hardly translate local information into end-to-end measurements. The increase in the complexity of networks as is the case of wireless mesh networks will not ease the life of users and operators. The purpose of our work in this direction is to study to which extent one can troubleshoot the current Internet and estimate the quality at the access either with end-to-end solutions or core network solutions. Our aim is to propose an architecture that allows end-users by collaborating together to infer the reasons for service degradation and to estimate the quality of access they perceive. This architecture can be purely end-to-end or can rely on some information from the core of the network as BGP routing information. We will build on this study to understand the limitations in the current Internet architecture and propose modifications that will ease the troubleshooting and make it more efficient in future network architectures. The proposed architecture will be the subject of validation over large scale experimental platforms as PlanetLab and OneLab.

## Experimental Environment for future Internet architecture

The Internet is relatively resistant to fundamental change (differentiated services, IP multicast, and secure routing protocols have not seen wide-scale deployment). A major impediment to deploy these services is the need for coordination: an Internet service provider (ISP) that deploys the service garners little benefit until other domains follow suit. Researchers are also under pressure to justify their work in the context of a federated network by explaining how new protocols could be deployed one network at a time, but emphasizing incremental deployability does not necessarily lead to the best architecture. In fact, focusing on incremental deployment may lead to solutions where each step along the path makes sense, but the end state is wrong. The substantive improvements to the Internet architecture may require fundamental change that is not incrementally deployable.

Network virtualisation has been proposed to support realistic large scale shared experimental facilities such as PlanetLab and GENI. We are working on this topic in the context of the European OneLab project.

Testing on PlanetLab has become a nearly obligatory step for an empirical research paper on a new network application or protocol to be accepted into a major networking conference or by the most prestigious networking journals. If one wishes to test a new video streaming application, or a new peer-to-peer routing overlay, or a new active measurement system for geo-location of internet hosts, hundreds of PlanetLab nodes are available for this purpose. PlanetLab gives the researcher login access to systems scattered throughout the world, with a Linux environment that is consistent across all of them.

However, network environments are becoming ever more heterogeneous. Third generation telephony is bringing large numbers of handheld wireless devices into the Internet. Wireless mesh and ad-hoc networks may soon make it common for data to cross multiple wireless hops while being routed in unconventional ways. For these new environments, new networking applications will arise. For their development and evaluation, researchers and developers will need the ability to launch applications on endhosts located in these different environments.

It is sometimes unrealistic to implement new network technology, for reasons that can be either technological - the technology is not yet available -, economical - the technology is too expensive -, or simply pragmatical - e.g. when actual mobility is key. For these kinds of situations, we believe it can be very convenient and powerful to resort to emulation techniques, in which real packets can be managed as if they had crossed, e.g., an ad hoc network.

In our project-team, we work to provide a realistic environment for the next generation of network experiments. Such a large scale, open, heterogeneous testbed should be beneficial to the whole networking academic and industrial community. It is important to have an experimental environment that increases the quality and quantity of experimental research outcomes in networking, and to accelerate the transition of these outcomes into products and services. These experimental platforms should be designed to support both research and deployment, effectively filling the gap between small-scale experiments in the lab, and mature technology that is ready for commercial deployment. As said above, in terms of experimental platforms, the well-known PlanetLab testbed is gaining ground as a secure, highly manageable, cost-effective world-wide platform, especially well fitted for experiments around New Generation Internet paradigms like overlay networks. The current trends in this field, as illustrated by the germinal successor known as GENI, are to address the following new challenges. Firstly, a more modular design will allow to achieve federation, i.e. a model where reasonably independent Management Authorities can handle their respective subpart of the platform, while preserving the integrity of the whole. Secondly, there is a consensus on the necessity to support various access and physical technologies, such as the whole range of wireless or optical links. It is also important to develop realistic simulators taking into account the tremendous growth in wireless networking, so to include the many variants of IEEE 802.11 networking, emerging IEEE standards such as WiMax (802.16), and cellular data services (GPRS, CDMA). While simulation is not the only tool used for data networking research, it is extremely useful because it often allows research questions and prototypes to be explored at many orders-of-magnitude less cost and time than that required to experiment with real implementations and networks.

Simulations allow a fast evaluation process, fully controlled scenarios, and reproducibility. However, they lack realism and the accuracy of the models implemented in the simulators is hard to assess. Emulation allows controlled environment and reproducibility, but it also suffers from a lack of realism. Experiments allow

more realistic environment and implementations, but they lack reproducibility and ease of use. Therefore, each evaluation technique has strengths and weaknesses. However, there is currently no way to combine them in a scientific experimental workflow. Typical evaluation workflows are split into four steps: topology description and construction, traffic pattern description and injection, trace instrumentation description and configuration, and, analysis based on the result of the trace events and the status of the environment during the experimentation. To achieve the integration of experimental workflows among the various evaluation platforms, the two following requirements must be verified:

- Reproducibility: A common interface for each platform must be defined so that a same script can be run transparently on different platforms. This also implies a standard way to describe scenarios, which includes the research objective of the scenario, topology description and construction, the description of the traffic pattern and how it is injected into the scenario, the description and configuration of the instrumentation, and the evolution of the environment during the experimentation
- Comparability: As each platform has different limitations, a way to compare the conclusions extracted from experiments run on different platforms, or on the same platform but with different conditions (this is in particular the case for the wild experimental platforms) must be provided.

Benchmarking is the function that provides a method of comparing the performance of various subsystems across different environments. Both reproducibility and comparability are essential to benchmarking. In order to facilitate the design of a general benchmarking methodology, we plan to integrate and automate a networking experiments workflow within the OneLab platform. This requires that we:

- Automate the definition of proper scenario definition taking in consideration available infra-structure to the experiment.
- Automate the task of mapping the experimentation topology on top of the available OneLab topology. We propose to first focus on a simple one-to-one node and link mapping the beginning.
- Define and provide extensive instrumentation sources within the OneLab system to allow users to gather all interesting trace events for offline analysis
- Measure and provide access to "environment variables" which measure the state of the OneLab system during an experimentation
- Define an offline analysis library which can infer experimentation results and comparisons based on traces and "environment variables".

To make the use of these components transparent, we plan to implement them within a simulation-like system which should allow experiments to be conducted within a simulator and within the OneLab testbed through the same programming interface. The initial version will be based on the ns-3 programming interface.

# 5. Software

## 5.1. ns-3

**Participant:** Daniel Camara [correspondant].

ns-3 is a discrete-event network simulator for Internet systems, targeted primarily for research and educational use. ns-3 is free software, licensed under the GNU GPLv2 license, and is publicly available for research, development, and use. ns-3 includes a solid event-driven simulation core as well as an object framework focused on simulation configuration and event tracing, a set of solid 802.11 MAC and PHY models, an IPv4, UDP, and TCP stack and support for nsc (integration of Linux and BSD TCP/IP network stacks).

See also the web page http://www.nsnam.org.

- Version: ns-3.7
- Keywords: networking event-driven simulation
- License: GPL (GPLv2)
- Type of human computer interaction: programmation C++/python, No GUI
- OS/Middleware: Linux, cygwin, osX
- Required library or software: standard C++ library: GPLv2
- Programming language: C++, python
- Documentation: doxygen

## 5.2. EphPub

**Participants:** Mohamed Ali Kaafar [correspondant], Claude Castelluccia.

EphPub (Ephemeral Publishing) (previously called EphCom) implements a novel key storage mechanism for time-bounded content, that relies on the caching mechanism of the Domain Name System (DNS). Features of EphPub include: EphPub exploits the fact that DNS servers temporarily cache the response to a recursive DNS query for potential further requests. EphPub provides higher security than Vanish, as it is immune to Sybil attacks. EphPub is easily deployable and does not require any additional infrastructure, such as Distributed Hash Tables. EphPub comes with high usability as it does not require users to install and execute any extra additional software. EphPub lets users define data lifetime with high granularity. We provide EphPub as an Android Application to provide ephemeral exchanged SMS, emails, etc. and as a Firefox or Thunderbird extensions so as to support ephemeral publication of any online document.
For more details about the different software products, see http://planete.inrialpes.fr/projects/ephemeral-publication/.

- Version: v0.1.2-beta
- ACM: K.4.1
- AMS: 94Axx
- Keywords: Ephemeral communications, Right to Forget, Future Internet Architecture, Privacy
- Software benefit: We provide a Firefox Extension that easily allows users to manage disappearing emails. We also provide a command-line tool to manage disappearing files.
- APP: Under APP deposit internal process
- License: GPL
- Type of human computer interaction: Firefox extension + Unix Console
- OS/Middelware: Firefox under any OS
- Required library or software: Python Ext
- Programming language: Python
- Documentation: No detailed documentation has been released so far. A detailed howto can be consulted however at: http://code.google.com/p/disappearingdata/source/browse/wiki/EphCOM_Firefox_Extension.wiki?r=77

## 5.3. Username Tester

**Participants:** Claude Castelluccia [correspondant], Mohamed Ali Kaafar, Daniele Perito.

Usernames are ubiquitous on the Internet. Almost every web site uses them to identify its users and, by design, they are unique within each service. In web services that have millions or hundreds of millions of users, it might become difficult to find a username that has not already been taken. For instance, you might have experienced that a specific username you wanted was already taken. This phenomenon drives users to choose increasingly complex and unique usernames.

We built a tool to estimate how unique and linkable usernames are and made it available on this page for you to check. For example, according to our tool, “ladygaga” or “12345678˝ only carry 24 and 17 bits of entropy, respectively. They are therefore not likely to be unique on the Internet. On the other hand, usernames such as “pdjkwerl” or “yourejerky” carry about 40 bits of entropy and are therefore very good identifiers.

Type your username (for example “zorro1982˝ or “dan.perito”) to discover how unique it is. This tool can help you to select an username that has low entropy and can’t be used to track you on the Internet.

Alternatively, try typing two usernames separated by a space. The tool will give an estimation on whether the two usernames are linkable. The tool is accessible here: http://planete.inrialpes.fr/projects/how-unique-are-your-usernames/

## 5.4. DroidMonitor

**Participants:** Claude Castelluccia [correspondant], Mohamed Ali Kaafar.

In nowadays world the technological progress evolves very quickly. There are more and more new devices, fully equipped with the latest innovations. The question is: do we adopt our main privacy concerns according to these new technologies as quickly as they grow and become widely available for us?...

We developed a novel tool, private data leakage monitoring tool, DroidMonitor. It aims to serve as an educational tool for regular Android Smartphones users to make them aware of existing privacy threats while they are using Location-Based Services. It can be downloaded here: http://planete.inrialpes.fr/android-privacy/

## 5.5. NEPI

**Participants:** Thierry Turletti [correspondant], Alina Quereilhac.

NEPI stands for Network Experimentation Programming Interface. NEPI implements a new experiment plane used to perform ns-3 simulations, planetlab and emulation experiments, and, more generally, any experimentation tool used for networking research. Its goal is to make it easier for experimenters to describe the network topology and the configuration parameters, to specify trace collection information, to deploy and monitor experiments, and, finally, collect experiment trace data into a central datastore. NEPI is a python API (with an implementation of that API) to perform all the above-mentioned tasks and allows users to access these features through a simple yet powerful graphical user interface called NEF.

During the year 2012 we improved support for PlanetLab experiments in NEPI, adding the ability to create customized routing overlays on top of PlanetLab. Details on these improvements can be found in [48]. We also included the ability to easily conduct CCNx http://www.ccnx.org/ experiments using PlanetLab nodes. This work was presented at the CCNx 2012 community meeting [73], and has had a good impact on the number of NEPI users.

Additionally, ongoing work on the context of the Openlab, Fed4Fire and Simulbed projects, has lead to a number of interesting extensions to NEPI. We are currently developing support to conduct experiments on OMF wireless testbeds (http://mytestbed.net/). We are also working to support DCE enabled experimentation, using the ns-3 simulator, in NEPI. Furthermore, recent work on improving NEPI’s experiment control architecture, to enable both easier extension to new experimentation platforms and improve the user ability to control of experiment tasks, was presented at the CoNEXT’12 Students Workshop (see [61]).

For more information, see also the web page http://nepi.inria.fr.

- Version: 2.0
- ACM: C.2.2, C.2.4
- Keywords: networking experimentation
- License: GPL (2)
- Type of human computer interaction: python library, QT GUI
- OS/Middelware: Linux
- Required library or software: python – http://www.python.org – http://rpyc.sourceforge.net
- Programming language: python

## 5.6. Reference implementation for SFA Federation of experimental testbeds

**Participants:** Thierry Parmentelat [correspondant], Julien Tribino.

We are codevelopping with Princeton University a reference implementation for the Testbed-Federation architecture known as SFA for Slice-based Federation Architecture. During 2011 we have focused on the maturation of the SFA codebase, with several objectives in mind, better interoperabity between the PlanetLab world and the EmuLab, a more generic shelter that other testbeds can easily leverage in order to come up with their own SFA-compliant wrapper and support for 'reservable' mode, which breaks the usual best-effort PlanetLab model. For more details about this contribution see section

See also the web page http://planet-lab.eu

- Version: myplc-5.0-rc26
- Keywords: networking testbed virtual machines
- License: Various Open Source Licences
- Type of human computer interaction: Web-UI, XMLRPC-based API, Qt-based graphical client
- OS/Middelware: Linux-Fedora
- Required library or software: Fedora-14 for the infrastructure side; the software comes with a complete software suite for the testbed nodes
- Programming languages: primarily python, C, ocaml
- Documentation: most crucial module plcapi is self-documented using a local format & related tool. See e.g. https://www.planet-lab.eu/db/doc/PLCAPI.php
- Codebase: http://git.onelab.eu

## 5.7. SfaWrap

**Participants:** Thierry Parmentelat [correspondant], Mohamed Larabi.

The SfaWrap is a reference implementation of the Slice-based Federation Architecture (SFA), the emerging standard for networking experimental testbed federation. We are codeveloping the SfaWrap with Princeton University, and during 2012, we have focused on:

- Participating in the discussions about the future and evolutions of the architecture of SFA, as part of the architecture working group of the GENI project.
- Turning this initially Planet-Lab specific implementation into a generic one, that testbed providers can easily leverage for bringing SFA-compliance to their own testbeds.
- Supporting the allocation and provisioning of both 'Exclusive' and 'Shared' testbed resources.
- Enlarging the federation scheme by federating various testbeds with heterogeneous resources, in order to allow researchers to combine all available resources and run advanced networking experiments of significant scale and diversity.
- Version: sfa-2.1-22, myplc-5.0-rc33
- Keywords: networking testbed federation
- License: Various Open Source Licenses
- Type of human computer interaction: Web-UI, XMLRPC-based API, Qt-based graphical client
- OS/Middelware: Linux
- Required library or software: python2.5 or superior
- Programming languages: python
- Documentation: http://svn.planet-lab.org/#SFAUser-leveldocumentation
- Codebase: http://git.onelab.eu/?p=sfa.git;a=summary

## 5.8. MultiCast Library Version 3

**Participant:** Vincent Roca [correspondant].

MultiCast Library Version 3 is an implementation of the ALC (Asynchronous Layered Coding) and NORM (NACK-Oriented Reliable Multicast Protocol) content delivery Protocols, and of the FLUTE/ALC file transfer application. This software is an implementation of the large scale content distribution protocols standardized by the RMT (Reliable Multicast Transport) IETF working group and adopted by several standardization organizations, in particular 3GPP for the MBMS (Multimedia Broadcast/Multicast Service), and DVB for the CBMS (Convergence of Broadcast and Mobile Services). Our software is used in operational, commercial environments, essentially in the satellite broadcasting area and for file delivery over the DVB-H system where FLUTE/ALC has become a key component. See http://planete-bcast.inrialpes.fr/ for more information.

## 5.9. OpenFEC.org: because open, free AL-FEC codes and codecs matter

**Participants:** Vincent Roca [correspondant], Jonathan Detchart [engineer], Ferdaouss Mattoussi [PhD student].

The goals of the OpenFEC.org http://openfec.org are:

1. to share IPR-free, open, AL-FEC codes,
2. to share high performance, ready-to-use, open, free, C-language, software codecs
3. to share versatile and automated performance evaluation environments.

This project can be useful to users who do not want to know the details of AL-FEC schemes but do need to use one of them in the software they are designing, or by users who want to test new codes or new encoding or decoding techniques, and who do know what they are doing and are looking for, or by users who need to do extensive tests for certain AL-FEC schemes in a given use-case, with a well defined channel model.

## 5.10. BitHoc

**Participants:** Chadi Barakat [correspondant], Thierry Turletti.

BitHoc (BitTorrent for wireless ad hoc networks) enables content sharing among spontaneous communities of mobile users using wireless multi-hop connections. It is an open source software developed under the GPLv3 licence. A first version of BitHoc has been made public. We want BitHoc to be the real testbed over which we evaluate our solutions for the support and optimization of file sharing in a mobile wireless environment where the existence of an infrastructure is not needed. The proposed BitHoc architecture includes two principal components: a membership management service and a content sharing service. In its current form it is composed of PDAs and smartphones equipped with WIFI adapters and Windows Mobile 6 operating system.

See also the web page http://planete.inria.fr/bithoc

- Version: 1.2
- Keywords: Tracker-less BitTorent for mobile Ad Hoc networks
- License: GPL (GPLv3)
- Type of human computer interaction: Windows Mobile 6 GUI
- OS/Middelware: Windows Mobile 6
- Required library or software: OpenSSL(http://www.openssl.org/, GPL), C++ Sockets, GPL)
- Programming languages: C++, C#
- Documentation: doxygen

## 5.11. TICP

**Participant:** Chadi Barakat [correspondant].

TICP is a TCP-friendly reliable transport protocol to collect information from a large number of network entities. The protocol does not impose any constraint on the nature of the collected information: availability of network entities, statistics on hosts and routers, quality of reception in a multicast session, weather monitoring, etc. TICP ensures two main things: *(i)* the information to collect arrives entirely and correctly to the collector where it is stored and forwarded to upper layers, and *(ii)* the implosion at the collector and the congestion of the network are avoided by controlling the rate of sending probes. The congestion control part of TICP is designed with the main objective to be friendly with applications using TCP. Experimental results show that TICP can achieve better performance than using parallel TCP connections for the data collection. The code of TICP is available upon request, it is an open source software under the GPLv3 licence.

See also the web page http://planete.inria.fr/ticp/

- Version: 1.0
- Keywords: Information Collection, Congestion and Error Control
- License: GPL (GPLv3)
- Type of human computer interaction: XML file
- OS/Middelware: Linux/Unix
- Required library or software: C/C++ Sockets
- Programming languages: C/C++
- Documentation: Text

## 5.12. Private Data Publication

**Participants:** Gergely Acs, Claude Castelluccia.

We are developing a set of tools to privately publish different types of datasets. For example, we are developing a software that can be used to sanitize sequential data (described in our CCS paper [41]). The code generates the set of noisy n-grams and generate a synthetic, and private, dataset. We are also developing a tool that implement the histogram sanitization algorithm described in our ICDM paper [33].

These tools are accessible here: http://planete.inrialpes.fr/projects/p-publication/

## 5.13. Experimentation Software

**ACQUA**

ACQUA stands for Application for Collaborative Estimation of the Quality of Internet Access. It has been developed within the French National project ANR CMON on Collaborative Monitoring in conjunction with Grenouille.com. ACQUA consists of a tool that lets the user have an estimation of the anomalies of the Internet based on active measurements of end-to-end delay metrics among a predefined set of landmarks (i.e. test points). When an anomaly is detected it is expressed in terms of how many destinations are affected by this anomaly, and how important in terms of delay variation is this anomaly for these affected destinations. See also http://planete.inria.fr/acqua/ for more information and for a java version of the code.

**WisMon**

WisMon is a Wireless Statistical Monitoring tool that generates real-time statistics from a unified list of packets, which come from possible different probes. This tool fulfills a gap on the wireless experimental field: it provides physical parameters on realtime for evaluation during the experiment, records the data for further processing and builds a single view of the whole wireless communication channel environment. WisMon is available as open source under the Cecill license, at http://planete.inria.fr/software/WisMon/.

**WEX Toolbox**

The Wireless Experimentation (WEX) Toolbox aims to set up, run and make easier the analysis of wireless experiments. It is a flexible and scalable open-source set of tools that covers all the experimentation steps, from the definition of the experiment scenario to the storage and analysis of results. Sources and binaries of the WEX Toolbox are available under the GPLv2 licence at https://twiki-sop.inria.fr/twiki/bin/view/Projets/Planete/WEXToolkit. WEX Toolbox includes the CrunchXML utility, which aims to make easier the running and the analysis of wireless experimentations. In a nutshell, it implements an efficient synchronization and merging algorithm, which takes XML (or PDML) input trace files generated by multiple probes, and stores only the packets fields that have been marked as relevant by the user in a MySQL database –original pcap traces should be first formatted in XML using wireshark. These operations are done in a smart way to balance the CPU resources between the central server (where the database is created) and the different probes (i.e., PC stations where the capture traces are located). CrunchXML is available under the GNU General Public License v2 at http://twiki-sop.inria.fr/twiki/bin/view/Projets/Planete/CrunchXML.

**WiMAX ns-3**

This simulation module for the ns-3 network simulator is based on the IEEE 802.16-2004 standard. It implements the PMP topology with TDD mode and aims to provide detailed and standard compliant implementation of the standard, supporting important features including QoS scheduling services, bandwidth management, uplink request/grant scheduling and the OFDM PHY layer. The module is available under the GNU General Public License at http://code.nsnam.org/iamine/ns-3-wimax. It will be included in the official 3.8v release of ns-3.

**MonLab**

Monitoring Lab is a platform for the emulation and monitoring of traffic in virtual ISP networks. It is supported by the FP7 ECODE project and is available for download at the web page of the tool http://planete.inria.fr/MonLab/ under the terms of the GPL licence. MonLab presents a new approach for the emulation of Internet traffic and for its monitoring across the different routers of the emulated ISP network. In its current version, the traffic is sampled at the packet level in each router of the platform, then monitored at the flow level. We put at the disposal of users real traffic emulation facilities coupled to a set of libraries and tools capable of Cisco NetFlow data export, collection and analysis. Our aim is to enable running and evaluating advanced applications for network wide traffic monitoring and optimization. The development of such applications is out of the scope of this research. We believe that the framework we are proposing can play a significant role in the systematic evaluation and experimentation of these applications' algorithms. Among the direct candidates figure algorithms for traffic engineering and distributed anomaly detection. Furthermore, methods for placing monitors, sampling traffic, coordinating monitors, and inverting sampling traffic will find in our platform a valuable tool for experimentation.

**MobiTrade**

MobiTrade is the ns-3 and Android implementation of our solution for trading content between wireless devices. The application provides a utility driven trading system for efficient content dissemination on top of a disruption tolerant network. While simple tit-for-tat (TFT) mechanisms can force nodes to *give one to get one*, dealing with the inherent tendency of peers to take much but give back little, they can quickly lead to deadlocks when some (or most) of interesting content must be somehow fetched across the network. To resolve this, MobiTrade proposes a trading mechanism that allows a node (*merchant*) to buy, store, and carry content for other nodes (its *clients*) so that it can later trade it for content it is personally interested in. To exploit this extra degree of freedom, MobiTrade nodes continuously profile the type of content requested and the collaboration level of encountered devices. An appropriate utility function is then used to collect an optimal inventory that maximizes the expected value of stored content for future encounters, matched to the observed mobility patterns, interest patterns, and collaboration levels of encountered nodes. See also http://planete.inria.fr/MobiTrade.

# 6. New Results

## 6.1. Towards Data-Centric Networking

**Participants:** Chadi Barakat, Damien Saucez, Jonathan Detchart, Mohamed Ali Kaafar, Ferdaouss Mattoussi, Marc Mendonca, Xuan-Nam Nguyen, Vincent Roca, Thierry Turletti.

- **DTN**

  Delay Tolerant Networks (DTNs) stand for wireless networks where disconnections may occur frequently. In order to achieve data delivery in such challenging environments, researchers have proposed the use of store-carry-and-forward protocols: there, a node may store a message in its buffer and carry it along for long periods of time, until an appropriate forwarding opportunity arises. Multiple message replicas are often propagated to increase delivery probability. This combination of long-term storage and replication imposes a high storage and bandwidth overhead. Thus, efficient scheduling and drop policies are necessary to: *(i)* decide on the order by which messages should be replicated when contact durations are limited, and *(ii)* which messages should be discarded when nodes' buffers operate close to their capacity.

  We worked on an optimal scheduling and drop policy that can optimize different performance metrics, such as the average delivery rate and the average delivery delay. First, we derived an optimal policy using global knowledge about the network, then we introduced a distributed algorithm that collects statistics about network history and uses appropriate estimators for the global knowledge required by the optimal policy, in practice. At the end, we are able to associate to each message inside the network a utility value that can be calculated locally, and that allows to compare it to other messages upon scheduling and buffer congestion. Our solution called HBSD (History Based Scheduling and Drop) integrates methods to reduce the overhead of the history-collection plane and to adapt to network conditions. The first version of HBSD and the theory behind have been published in 2008. A recent paper [27] provides an extension to a heterogenous mobility scenario in addition to refinements to the history collection algorithm. An implementation is proposed for the DTN2 architecture as an external router and experiments have been carried out by both real trace driven simulations and experiments over the SCORPION testbed at the University of California Santa Cruz. We refer to the web page of HBSD for more details http://planete.inria.fr/HBSD_DTN2/.

  HBSD in its current version is for point-to-point communications. Another interesting schema is to consider one-to-many communications, where requesters for content express their interests to the network, which looks for the content on their behalf and delivers it back to them. Along the main ideas of HBSD, we worked on a content optimal-delivery algorithm, CODA, that distributes content to multiple receivers over a DTN. CODA assigns a utility to each content item published in the network; this value gauges the contribution of a single content replica to the network's overall delivery-rate. CODA performs buffer management by first calculating the delivery-rate utility of each cached content-replica and then discarding the least-useful item. When an application requests content, the node supporting the application will look for the content in its cache. It will immediately deliver it to the application if the content is stored in memory. In case the request cannot be satisfied immediately, the node will store the pending request in a table. When the node meets another device, it will send the list of all pending requests to its peer; the peer device will try to satisfy this list by sending the requester all the matching content stored in its own buffer. A meeting between a pair of devices might not last long enough for all requested content to be sent. We address this problem by sequencing transmissions of data in order of decreasing delivery-rate utility. A content item with few replicas in the network has a high delivery rate utility; these items must be transmitted first to avoid degrading the content delivery-rate metric. The node delivers the requested content to the application as soon as it receives it in its buffer. We implement CODA over the CCNx protocol, which provides the basic tools for requesting, storing, and forwarding content. Detailed information on CODA and the implementation work carried out herein can be found in [76].

- **Naming and Routing in Content Centric Networks**

  Content distribution prevails in todays Internet and content oriented networking proposes to access data directly by their content name instead of their location, changing so the way routing must be conceived. We proposed a routing mechanism that faces the new challenge of interconnecting content-oriented networks. Our solution relies on a naming resolution infrastructure that provides the binding between the content name and the content networks that can provide it. Content-oriented messages are sent encaspulated in IP packets between the content-oriented networks. In order to allow scalability and policy management, as well as traffic popularity independence, binding requests are always transmitted to the content owner. The content owner can then dynamically learn the caches in the network and adapt its binding to leverage the cache use.

  The work done so far is related to routing between content-oriented networks. We are starting an activity on how to provide routing inside a content network. To that aim, we are investigating on the one hand probabilistic routing and, on the other hand, deterministic routing and possible extension to Bellman-Ford techniques. In addition to routing, we are investigating the problem of congestion in content-oriented networks. Indeed, in this new paradigm, congestion must be controlled on a per-hop basis, as opposed to the end-to-end congestion control that prevails today. We think that we can combine routing and congestion control to optimize resource consumption. Finally, we are studying the implications of using CCN from an economical perspective. See [100] for more details.

- **On the fairness of CCN**

  Content-centric networking (CCN) is a new paradigm to better handle contents in the future Internet. Under the assumption that CCN networks will deploy a similar congestion control mechanism than in today's TCP/IP (i.e., AIMD), we built an analytical model of the bandwidth sharing in CCN based on the "square-root formula of TCP". With this model we can compare CCN download performance to what users get today. We consider different factors such as the way CCN routers are deployed, the popularity of contents, or the capacity of links and observe that when AIMD is used in a CCN network less popular content throughput is massively penalised whilst the individual gain for popular content is negligible. Finally, the main advantage of using CCN is the decrease of load at the server side. Our observations advocate the necessity to clearly define the notion of fairness in CCN and to design a proper congestion control to avoid less popular contents to become hardly accessible in tomorrow's Internet.

  Our results [75] clearly point to a fairness issue if AIMD is used with CCN. Indeed, combining blindly AIMD and CCN can severely worsen the download throughput of less popular contents with respect to the today's Internet due to subtle interactions with in-network caching strategies. The way cache memories are distributed within chain topologies has been investigated too, showing that for small and heterogeneous cache spaces, placing the biggest caches close to clients improves performance due to a smaller RTT on average. On the other hand, CCN can significantly reduce the load at the server side independently of the cache allocation strategy. Our findings advocate the urge of clearly defining the notion of fairness in CCN and designing congestion control algorithms able to limit the unfairness observed between contents of different popularities. The work is currently used within the IRTF ICNRG research group in order to motivate and define an appropriate congestion control mechanism for information centric networks like CCN. Moreover, we are currently validating the analytical results with an implementation of CCN where we can evaluate how much our model deviates from the reality when contents are of various size or small. The implementation will also be a support to test different congestion control mechanism.

- **CCN to enable profitable collaborative OTT services**

The ubiquity of broadband Internet and the proliferation of connected devices like laptops, tablets, or TV result in a high demand of multimedia content such as high definition video on demand (VOD) for which the Internet has been poorly designed with the Internet Protocol (IP). Information-Centric Networking and more precisely Content Centric Networking (CCN) overtake the limitation of IP by considering content as the essential element of the network instead of the topology. CCN and its content caching capabilities is particularly adapted to Over-The-Top (OTT) services like Netflix, Hulu, Xbox Live, or YouTube that distribute high-definition multimedia content to millions of consumers, independently of their location. However, bringing content as the most important component of the network implies fundamental changes in the Internet and the transition to a fully CCN Internet might take a long time. Despite this transition period where CCN and IP will co-exist, we have shown that OTT service providers and consumers have strong incentives for migrating to CCN. We also propose a transition mechanism based on the Locator/Identifier Separation Protocol (LISP) [28] that allows the provider to track the demands from its consumers even though they do not download the contents from another consumers instead of the producer itself.

CCN, compared to IP, provides better security and performance. This last point is very interesting for OTT service providers that deliver multimedia content where performance is a key factor for the adoption of the service by consumers. With CCN, the content can be retrieved from the caches in the different CCN islands, instead of always being delivered by the content publisher. As a result, content retrieval is faster for the consumer and the operational cost of the publisher is reduced. Moreover, as the content is cached by the consumers and because the consumer can provide the content to other consumers, the overall performance increases with the number of consumers instead of decreasing as it is the case in IP today where the content is delivered by the hosting server. This property is particularly interesting because it dampens the effect of flash crowds which are normally very costly for OTT service providers as they have to provision their servers and networks to support them. Using CCN with caching at the consumers has then a direct impact on the profit earned by the OTT service provider as its costs are reduced. However, to benefit from the caching capabilities of consumers, the producer must propose real incentives to its consumers to *collaborate* and cache the content. To understand how incentives can be provided, it is necessary to remember that content in OTT is provided either freely to the consumer or in exchange of a fee. When the content is provided freely, the incomes for the publisher are ensured by advertisements dispersed in the content (e.g., banner, commercial interruptions...). A consumer has incentives to collaborate with the system if it receives some sort of discount, expressed in advertisement reduction or fee reduction. On the one hand, the discount has a cost for the publisher as its revenues will be reduced. On the other hand, the collaboration from its consumers reduces its operational costs. Hence, the publisher must determine the optimal discount, such that it maximises its profit. The situation for the consumer is the exact opposite: its costs are increasing because it is providing content to other consumers but its revenues also increase as it receives a discount on its expenses. We have determined the conditions to respect when deploying OTT with loosely collaborative consumers [99]. We currently refine the results using game theory.

- **Software-Defined Networking in Heterogeneous Networked Environments**

  Software-Defined Networking (SDN) has been proposed as a way to facilitate network evolution by allowing networks and their infrastructure to be programmable. In the context of the COMMUNITY associated team with University of California Santa Cruz (see URL http://inrg.cse.ucsc.edu/community/) , we are studying the potential of SDN to facilitate the deployment and management of new architectures and services in heterogeneous environments. In particular, we focus on the fundamental issues related to enabling SDN in infrastructure-less/decentralized networked environments and we use OpenFlow as our target SDN platform. Our plan is to develop a hybrid SDN framework

that strikes a balance between a completely decentralized approach like Active Networking and a centralized one such as OpenFlow~[58].

We are also currently evaluating the efficiency of SDN for optimizing caching in content-centric networks. CCN advocates in-network caching, i.e., to cache contents on the path from content providers to requesters. Akthough this on-path caching achieves good overall performance, we have shown that this strategy is far from being the optimal inside a domain. On this purpose, we proposed the notion of off-path caching by allowing deflection of the most popular traffic off the optimal path towards off-path caches available across the domain[100]. Off-path caching improves the global hit ratio and permits to reduce the peering links' bandwidth usage. We are now investigating whether SDN functionalities can be used to implement this optimal caching technique, in particular to identify of the most popular contents, and to configure deflection mechanisms within routers~[94].

- **Application-Level Forward Error Correction Codes (AL-FEC) and their Applications to Broadcast/Multicast Systems**

  With the advent of broadcast/multicast systems (e.g., 3GPP MBMS services), large scale content broadcasting is becoming a key technology. This type of data distribution scheme largely relies on the use of Application Level Forward Error Correction codes (AL-FEC), not only to recover from erasures but also to improve the content broadcasting scheme itself (e.g., with FLUTE/ALC).

  Our LDPC-Staircase codes, that offer a good balance in terms of performance, have been included as the primary AL-FEC solution for ISDB-Tmm (Integrated Services Digital Broadcasting, Terrestrial Mobile Multimedia), a Japanese standard for digital television (DTV) and digital radio, with a commercial service that started in April 2012. This is the first adoption of these codes in an international standard. These codes, along with our FLUTE/ALC software, are now part of the server and terminal protocol stack: http://www.rapidtvnews.com/index.php/2012041721327/ntt-data-mse-and-expways-joint-solution-powers-japanese-mobile-tv-service.html.

  This success has been made possible, on the one hand, by major efforts in terms of standardization within IETF: the RFC 5170 (2008) defines the codes and their use in FLUTE/ALC, a protocol stack for massively scalable and reliable content delivery services, an active Internet-Draft published last year describes the use of these AL-FEC codes in FECFRAME, a framework for robust real-time streaming applications, and recent Internet-Drafts [91][92] define the GOE (Generalized Object Encoding) extension of LDPC-Staircase codes for UEP (Unequal Erasure Protection) and file bundle protection services.

  This success has also been made possible, on the other hand, by our efforts in terms of design and evaluation of two efficient software codecs for LDPC-Staircase codes. One of them is distributed in open-source, as part of our OpenFEC project (http://openfec.org), a unique initiative that aims at promoting open and free AL-FEC solutions. The second one, a highly optimized version with improved decoding speed and reduced memory requirements, is commercialized through an industrial partner, Expway.

  Since May 2012, along with the Expway French company, we are proposing the Reed-Solomon + LDPC-Staircase codes for the 3GPP-eMBMS call for technology, as a candidate for next generation AL-FEC codes for multimedia services. We have shown that these codes offer very good erasure recovery capabilities, in line with 3GPP requirements, and extremely high decoding speeds, usually significantly faster than that of the other proposals. The final decision is expected for end of January 2013. In any case we have once again showed that these codes provide very good performance, often ahead of the competitors, and an excellent balance between several technical and non technical criteria.

Finally our activities in the context of the PhD of F. Mattoussi include the design, analysis and improvement of GLDPC-Staircase codes, a "Generalized" extension to LDPC-Staircase codes. We have shown in particular that these codes: (1) offer small rate capabilities, i.e. can produce a large number of repair symbols 'on-the-fly', when needed; (2) feature high erasure recovery capabilities, close to that of ideal codes. Therefore they offer a nice opportunity to extend the field of application of existing LDPC-Staircase codes (IETF RFC 5170), while keeping backward compatibility (i.e. LDPC-Staircase "codewords" can be decoded with a GPLDPC-Staircase codec). More information is available in [56][57][55].

- **Unequal Erasure Protection (UEP) and File bundle protection through the GOE (Generalized Object Encoding) scheme**

  This activity has been initiated with the PostDoc work of Rodrigue IMAD. It focuses on Unequal Erasure Protection capabilities (UEP) (when a subset of an object has more importance than the remaing) and file bundle protection capabilities (e.g. when one want to globally protect a large set of small objects).

  After an in-depth understanding of the well-known PET (Priority Encoding Technique) scheme, and the UOD for RaptorQ (Universal Object Delivery) initiative of Qualcomm, which is a realization of the PET approach, we have designed the GOE FEC Scheme (Generalized Object Encoding) alternative. The idea, simple, is to decouple the FEC protection from the natural object boundaries, and to apply an independant FEC encoding to each "generalized object". The main difficulty is to find an appropriate signaling solution to synchronize the sender and receiver on the exact way FEC encoding is applied. In [91] we show this is feasible, while keeping a backward compatibility with receivers that do not support GOE FEC schemes. Two well known AL-FEC schemes have also been extended to support this new approach, with very minimal modifications, namely Reed-Solomon and LDPC-Staircase codes [92], [91].

  During this work, we compared the GOE and UOD/PET schemes, both from an analytical point of view (we use an N-truncated negative binomial distribution to that purpose) and from an experimental, simulation based, point of view [64]. We have shown that the GOE approach, by the flexibility it offers, its simplicity, its backward compatibility and its good recovery capabilities (under finite of infinite length conditions), outperforms UOD/PET for practical realizations of UEP/file bundle protection systems. See also http://www.ietf.org/proceedings/81/slides/rmt-2.pdf.

- **Application-Level Forward Error Correction Codes (AL-FEC) and their Applications to Robust Streaming Systems**

  AL-FEC codes are known to be useful to protect time-constrained flows. The goal of the IETF FECFRAME working group is to design a generic framework to enable various kinds of AL-FEC schemes to be integrated within RTP/UDP (or similar) data flows. Our contributions in the IETF context are three fold. First of all, we have contributed to the design and standardization of the FECFRAME framework, now published as a Standards Track RFC6363.

  Secondly, we have proposed the use of Reed-Solomon codes (with and without RTP encapsulation of repair packets) and LDPC-Staircase codes within the FECFRAME framework: [85] for Reed-Solomon and [88] for LDPC-Staircase. Both documents are close to being published as RFCs.

  Finally, in parallel, we have started an implementation of the FECFRAME framework in order to gain an in-depth understanding of the system. Previous results showed the benefits of LDPC-Staircase codes when dealing with high bit-rate real-time flows.

A second type of activity, in the context of robust streaming systems, consisted in the analysis of the Tetrys approach. Tetrys is a promising technique that features high reliability while being independent from RTT, and performs better than traditional block FEC techniques in a wide range of operational conditions.

- **A new File Delivery Application for Broadcast/Multicast Systems**

  FLUTE [95] has long been the one and only official file delivery application on top of the ALC reliable multicast transport protocol. However FLUTE has several limitations (essentially because the object meta-data are transmitted independently of the objects themselves, in spite of their inter-dependency), features an intrinsic complexity, and is only available for ALC.

  Therefore, we started the design of FCAST, a simple, lightweight file transfer application, that works both on top of both ALC and NORM [82]. This work is carried out as part of the IETF RMT Working Group, in collaboration with B. Adamson (NRL). This document has passed WG Last Call and is currently considered by IESG.

- **Security of the Broadcast/Multicast Systems**

  Sooner or later, broadcasting systems will require security services. This is all the more true as heterogeneous broadcasting technologies are used, some of them being by nature open, such as WiFi networks. Therefore, one of the key security services is the authentication of the packet origin and the packet integrity check. To that purpose, we have specified the use of simple authentication and integrity schemes (i.e., group MAC and digital signatures) in the context of the ALC and NORM protocols and the standard is now published as IETF RFC 6584 [98].

- **High Performance Security Gateways for High Assurance Environments**

  This work focuses on very high performance security gateways, compatible with 10Gbps or higher IPsec tunneling throughput, while offering a high assurance thanks in particular to a clear red/black flow separation. In this context we have studied last year the feasibility of high-bandwidth, secure communications on generic machines equipped with the latest CPUs and General-Purpose Graphical Processing Units (GPGPU).

  The work carried out in 2011-2012 consisted in setting up and evaluating the high performance platform. This platform heavily relies on the Click modular TCP/IP protocol stack implementation, which turned out to be a key enabler both in terms of specialization of the stack and parallel processing. Our activities also consisted in analyzing the PMTU discovery aspect since it is a critical factor in achieving high bandwidths. To that goal we have designed a new approach for qualifying ICMP blackholes in the Internet, since PMTUD heavily relies on ICMP [51].

## 6.2. Network Security and Privacy

**Participants:** Claude Castelluccia, Gergely Acs, Mathieu Cunche, Daniele Perito, Lukasz Olejnik, Mohamed Ali Kaafar, Abdelberi Chaabane, Cédric Lauradoux, Minh-Dung Tran.

- *Private Big Data Publication* Public datasets are used in a variety of applications spanning from genome and web usage analysis to location-based and recommendation systems. Publishing such datasets is important since they can help us analyzing and understanding interesting patterns. For example, mobility trajectories have become widely collected in recent years and have opened the possibility to improve our understanding of large-scale social networks by investigating how people exchange information, interact, and develop social interactions. With billion of handsets in use

worldwide, the quantity of mobility data is gigantic. When aggregated, they can help understand complex processes, such as the spread of viruses, and build better transportation systems, prevent traffic congestion. While the benefits provided by these datasets are indisputable, they unfortunately pose a considerable threat to individual privacy. In fact, mobility trajectories might be used by a malicious attacker to discover potential sensitive information about a user, such as his habits, religion or relationships. Because privacy is so important to people, companies and researchers are reluctant to publish datasets by fear of being held responsible for potential privacy breaches. As a result, only very few of them are actually released and available. This limits our ability to analyze such data to derive information that could benefit the general public. Here follows some recent results of our activities in this domain.

**Privacy-Preserving Sequential Data Publication [41]:** Sequential data is being increasingly used in a variety of applications, spanning from genome and web usage analysis to location-based recommendation systems. Publishing sequential data is of vital importance to the advancement of these applications since they can enable researchers to analyze and understand interesting sequential patterns. However, as shown by the re-identification attacks on the AOL and Netflix datasets, releasing sequential data may pose considerable threats to individual privacy. Recent research has indicated the failure of existing sanitization techniques to provide claimed privacy guarantees. It is therefore urgent to respond to this failure by developing new schemes with provable privacy guarantees. Differential privacy is one of the only models that can be used to provide such guarantees. Due to the inherent sequentiality and high-dimensionality, it is challenging to apply differential privacy to sequential data. In this work, we address this challenge by employing a variable-length n-gram model, which extracts the essential information of a sequential database in terms of a set of variable-length n-grams. Our approach makes use of a carefully designed exploration tree structure and a set of novel techniques based on the Markov assumption in order to lower the magnitude of added noise. The published n-grams are useful for many purposes. Furthermore, we develop a solution for generating a synthetic database, which enables a wider spectrum of data analysis tasks. Extensive experiments on real-life datasets demonstrate that our approach substantially outperforms the state-of-the-art techniques.

**Private Histogram Publishing [33]:**

Differential privacy can be used to release different types of data, and, in particular, histograms, which provide useful summaries of a dataset. Several differentially private histogram releasing schemes have been proposed recently. However, most of them directly add noise to the histogram counts, resulting in undesirable accuracy. In this work, we propose two sanitization techniques that exploit the inherent redundancy of real-life datasets in order to boost the accuracy of histograms. They lossily compress the data and sanitize the compressed data. Our first scheme is an optimization of the Fourier Perturbation Algorithm (FPA) presented in [13]. It improves the accuracy of the initial FPA by a factor of 10. The other scheme relies on clustering and exploits the redundancy between bins. Our extensive experimental evaluation over various real-life and synthetic datasets demonstrates that our techniques preserve very accurate distributions and considerably improve the accuracy of range queries over attributed histograms.

- *Privacy Issues on the Internet* Internet users are being increasingly tracked and profiled. Companies utilize profiling to provide customized, i.e. personalized services to their customers, and hence increase revenues.

  **Privacy issues of Targeted Advertising [37]:** Behavioral advertising takes advantage from profiles of users' interests, characteristics (such as gender, age and ethnicity) and purchasing activities. For example, advertising or publishing companies use behavioral targeting to display advertisements that closely reflect users' interests (e.g. 'sports enthusiasts'). Typically, these interests are inferred from users' web browsing activities, which in turn allows building of users' profiles. It can be argued that customization resulting from profiling is also beneficial to users who receive useful information and relevant online ads in line with their interests. However, behavioral targeting is often perceived as a

threat to privacy mainly because it heavily relies on users' personal information, collected by only a few companies. In this work, we show that behavioral advertising poses an additional privacy threat because targeted ads expose users' private data to any entity that has access to a small portion of these ads. More specifically, we show that an adversary who has access to a user's targeted ads can retrieve a large part of his interest profile. This constitutes a privacy breach because interest profiles often contain private and sensitive information.

**On the Uniqueness of Web Browsing History Patterns [60]:** We present the results of the first large-scale study of the uniqueness of Web browsing histories, gathered from a total of $368,284$ Internet users who visited a history detection demonstration website. Our results show that for a majority of users (69%), the browsing history is unique and that users for whom we could detect at least 4 visited websites were uniquely identified by their histories in $97\%$ of cases. We observe a high rate of stability in browser history fingerprints: for repeat visitors, $80\%$ of fingerprints are identical over time, and differing ones were strongly correlated with original history contents, indicating static browsing preferences. We report a striking result that it is enough to test for a small number of pages in order to both enumerate users' interests and perform an efficient and unique behavioral fingerprint; we show that testing 50 web pages is enough to fingerprint $42\%$ of users in our database, increasing to $70\%$ with 500 web pages. Finally, we show that indirect history data, such as information about *categories* of visited websites can also be effective in fingerprinting users, and that similar fingerprinting can be performed by common script providers such as Google or Facebook.

- **Adaptive Password-Strength Meters from Markov Models [38]**

  Passwords are a traditional and widespread method of authentication, both on the Internet and off-line. Passwords are portable, easy to understand for laypersons, and easy to implement for the operator. Thus, password-based authentication is likely to stay for the foreseeable future.

  To ensure an acceptable level of security of user-chosen passwords, sites often use mechanisms to test the strength of a password (often called *pro-active password checkers*) and then reject weak passwords. Hopefully this ensures that passwords are reasonably strong on average and makes guessing passwords infeasible or at least too expensive for the adversary. Commonly used password checkers rely on rules such as requiring a number and a special character to be used. However, as we will show and also has been observed in previous work, the accuracy of such password checkers is low, which means that often insecure passwords are accepted and secure passwords are rejected. This adversely affects both security and usability.

  In this work, we propose to use password strength meters based on Markov-models, which estimate the true strength of a password more accurately than rule-based strength meters. Roughly speaking, the Markov-model estimates the strength of a password by estimating the probability of the $n$-grams that compose said password. Best results can be obtained when the Markov-models are trained on the actual password database. We show, in this work, how to do so without sacrificing the security of the password database, even when the $n$-gram database is leaked.

  We show how to build secure adaptive password strength meters, where security should hold even when the $n$-gram database leaks. This is similar to traditional password databases, where one tries to minimize the effects of a database breach by hashing and salting the stored passwords. This is not a trivial task. One potential problem is that, particularly strong passwords, can be leaked entirely by an $n$-gram database (without noise added).

- **Fast Zero-Knowledge Authentication [47]** We explore new area/throughput trade-offs for the Girault, Poupard and Stern authentication protocol (GPS). This authentication protocol was selected in the NESSIE competition and is even part of the standard ISO/IEC 9798. The originality of our work comes from the fact that we exploit a fixed key to increase the throughput. It leads us to implement GPS using the Chapman constant multiplier. This parallel implementation is 40 times faster but 10 times bigger than the reference serial one. We propose to serialize this multiplier to reduce its area at the cost of lower throughput. Our hybrid Chapman's multiplier is 8 times faster but

only twice bigger than the reference. Results presented here allow designers to adapt the performance of GPS authentication to their hardware resources. The complete GPS prover side is also integrated in the network stack of the PowWow sensor which contains an Actel IGLOO AGL250 FPGA as a proof of concept.

- **Energy Efficient Authentication Strategies for Network Coding [26]**

  Recent advances in information theory and networking, e.g. aggregation, network coding or rateless codes, have significantly modified data dissemination in wireless networks. These new paradigms create new threats for security such as pollution attacks and denial of services (DoS). These attacks exploit the difficulty to authenticate data in such contexts. The particular case of xor network coding is considered herein. We investigate different strategies based on message authentication codes algorithms (MACs) to thwart these attacks. Yet, classical MAC designs are not compatible with the linear combination of network coding. Fortunately, MACs based on universal hash functions (UHFs) match nicely the needs of network coding: some of these functions are linear $h(x_1 \oplus x_2) = h(x_1) \oplus h(x_2)$. To demonstrate their efficiency, we consider the case of wireless sensor networks (WSNs). Although these functions can drastically reduce the energy consumption of authentication (up to 68% gain over the classical designs is observed), they increase the threat of DoS. Indeed, an adversary can disrupt all communications by polluting few messages. To overcome this problem, a group testing algorithm is introduced for authentication resulting in a complexity linear in the number of attacks. The energy consumption is analyzed for cross-point and butterfly network topologies with respect to the possible attack scenarios. The results highlight the trade-offs between energy efficiency, authentication and the effective throughput for the different MAC modes.

- **Towards Stronger Jamming Model: Application to TH-UWB Radio [35]**

  With the great expansion of wireless communications, jamming becomes a real threat.We propose a new model to evaluate the robustness of a communication system to jamming. The model results in more scenarios to be considered ranging from the favorable case to the worst case. The model is applied to a TH-UWB radio. The performance of such a radio in presence of the different jamming scenarios is analyzed. We introduce a mitigation solution based on stream cipher that restricts the jamming problem of the TH-UWB communication to the more favorable case while preserving confidentiality.

- **Privacy risks quantification in Online social networks**

  In this project, we analyze the different capabilities of online social networks and aim to quantify the privacy risks users are undertaking in this context. Online Social Networks (OSNs) are a rich source of information about individuals. It may be difficult to justify the claim that the existence of public profiles breaches the privacy of their owners, as they are the ones who entered the data and made them publicly available in the first place. However, aggregation of multiple OSN public profiles is debatably a source of privacy loss, as profile owners may have expected each profile's information to stay within the boundaries of the OSN service in which it was created. First we present an empirical study of personal information revealed in public profiles of people who use multiple Online Social Networks (OSNs). This study aims to examine how users reveal their personal information across multiple OSNs. We consider the number of publicly available attributes in public profiles, based on various demographics and show a correlation between the amount of information revealed in OSN profiles and specific occupations and the use of pseudonyms. Then, we measure the complementarity of information across OSNs and contrast it with our observations about users who share a larger amount of information. We also measure the consistency of information revelation patterns across OSNs, finding that users have preferred patterns when revealing information across OSNs. To evaluate the quality of aggregated profiles we introduce a consistency measure for attribute values, and show that aggregation also improves information granularity. Finally, we demonstrate how the availability of multiple OSN profiles can be exploited to improve the success of obtaining users' detailed contact information, by cross-linking with publicly available data sources such as online phone directories. This work has been published in ACM SIGCOMM WOSN [42].

In a second study, we examine the user tracking capabilities of the three major global Online Social Networks (OSNs). We study the mechanisms which enable these services to persistently and accurately follow users web activity, and evaluate to which extent this phenomena is spread across the web. Through a study of the top 10K websites, our findings indicate that OSN tracking is diffused among almost all website categories, independently from the content and from the audience. We also evaluate the tracking capabilities in practice and demonstrate by analyzing a real traffic traces that OSNs can reconstruct a significant portion of users web profile and browsing history. We finally provide insights into the relation between the browsing history characteristics and the OSN tracking potential, highlighting the high risk properties. This work has also been published in ACM SIGCOMM WOSN [40].

In a third study, we also analyzed the inference capabilities of third parties from seemingly harmless and unconsciously publicly shared data. Interests (or "likes") of users is one of the highly-available on-line information on the web. In this study, we show how these seemingly harmless interests (e.g., music interests) can leak privacy sensitive information about users. In particular, we infer their undisclosed (private) attributes using the public attributes of other users sharing similar interests. In order to compare user-defined interest names, we extract their semantics using an ontologized version of Wikipedia and measure their similarity by applying a statistical learning method. Besides self-declared interests in music, our technique does not rely on any further information about users such as friend relationships or group belongings. Our experiments, based on more than 104K public profiles collected from Facebook and more than 2000 private profiles provided by volunteers, show that our inference technique efficiently predicts attributes that are very often hidden by users. This is the first time that user interests are used for profiling, and more generally, semantics-driven inference of private data is addressed. Our work received many media attention and was published in the prestigious NDSS symposium [39].

- **On the Privacy threats of hidden information in Wireless communication**

  Wi-Fi protocol has the potential to leak personal information. Wi- Fi capable devices commonly use active discovery mode to find the available Wi-Fi access points (APs). This mechanism includes broadcast of the AP names to which the mobile device has previously been connected to, in plain text, which may be easily observed and captured by any Wi-Fi device monitoring the control traffic. The combination of the AP names belonging to any mobile device can be considered as a Wi-Fi fingerprint, which can be used to identify the mobile device user. Our research investigates how it is possible to exploit these fingerprints to identify links between users i.e. owners of the mobile devices broadcasting such links. In this project, we have used an approach based on the similarity between the Wi-Fi fingerprints, which is equated to the likelihood of the corresponding users being linked. When computing the similarity between two Wi-Fi fingerprints, two dimensions need to be considered : (i) The number of network names in common. Indeed, sharing a network is an indication of the existence of a link, e.g. friends and family that share multiple Wi-Fi networks. (ii) The rarity of the network names in common. Some network names are very common and sharing them does not imply a link between the users. This is the case for public network names such as McDonalds Free Wi-Fi, or default network names such as NETGEAR and Linksys. On the other hand, uncommon network names such as Griffin Family Network or Orange-3EF50 are likely to indicate a strong link between the users of these networks. Utilising a carefully designed similarity metric, we have been able to infer the existence of social links with a high confidence: 80% of the links were detected with an error rate of 7%. We show that through real-life experiments that owners of smartphones are particularly exposed to this threat, as indeed these devices are carried on persons throughout the day, connecting to multiple Wi-Fi networks and also broadcasting their connection history. There are a number of industry and research initiatives aiming to address Wi-Fi related privacy issues. The deployment of new technology i.e. privacy preserving discovery services, would necessitate software modifications in currently deployed APs and devices. The obvious solution to disable active discovery mode, comes at the expense of performance and usability, i.e. with an extended time duration for the Wi-Fi capable device to find and connect to an available AP. As a

possible first step, users should be encouraged to remove the obsolete connection history entries, which may lower the similarity metric and thus reduce the ease of linkage. Our papers illustrating this study have been presented in the WoWMoM'12 conference [45] and in the IEEE MILCOM conference [43].

- **Information leakage in Ads networks**

  In targeted (or behavioral) advertising, users' behaviors are tracked over time in order to customize served ads to their interests. This creates serious privacy concerns since for the purpose of profiling, private information is collected and centralized by a limited number of companies. Despite claims that this information is secure, there is a potential for this information to be leaked through the customized services these companies are offering. In this study, we show that targeted ads expose users' private data not only to ad providers but also to any entity that has access to users' ads. We propose a methodology to filter targeted ads and infer users' interests from them. We show that an adversary that has access to only a small number of websites containing Google ads can infer users' interests with an accuracy of more than 79% (Precision) and reconstruct as much as 58% of a Google Ads profile in general (Recall). This study is the first work that identifies and quantifies information leakage through ads served in targeted advertising. We published a paper illustrating these results in the prestigious Privacy Enhancing Technologies Symposium PETS 2012 [37].

- **Privacy in P2P file sharing systems**

  In this study, we aim at characterizing anonymous file sharing systems from a privacy perspective. We concentrate on a recently deployed privacy-preserving file sharing system: OneSwarm. Our characterisation is based on measurement of several aspects of the OneSwarm system such as the nature of the shared and searched content and the geolocation and number of users. Our findings indicate that, as opposed to common belief, there is no significant difference in downloaded content between this system and the classical BitTorrent ecosystem. We also found that a majority of users appear to be located in countries where anti-piracy laws have been recently adopted and enforced (France, Sweden and U.S). Finally, we evaluate the level of privacy provided by OneSwarm, and show that, although the system has strong overall privacy, a collusion attack could potentially identify content providers. This work has been published in [46].

- **Privacy leakage on mobile devices: the Mobilitics Inria-CNIL project**

  This joint Inria-CNIL (the French data protection agency) project aims at assessing the privacy risks associated to the use of smartphones and tablets, in particular because of personal information leakage to remote third parties. Both applications and the base OS services are considered as potential source of information leakage. More precisely, the goals are to define a platform and a methodology to identify, measure, and see the evolution over the time of privacy risks.

  If similar risks exist with a PC, the situation is more worrying with mobile terminals. The reasons are:

  - the intrusive feature of these terminals that their owner continuously keep with them;
  - the amount of personnal information available on these terminals (mobile terminals aggregate personnal information but also create them, for instance with geolocalisation information);
  - the facility with which the owner can personnalize its terminal with new applications;
  - the financial incentives that lead companies to collect and use personnal information;
  - the fact that the terminal user has no tool (e.g. a "privacy" firewall) to control precisely what information is exchanged with whom. The permissions provided by Android is too coarse grained to be useful, and the new privacy dashboard of IOS 6 does not enable the user to have an idea of how personnal information is used by an authorized application (a one time access to a personnal information and local processing within the application can be acceptable, whereas the periodic transmission of this information to remote servers is not);

The final goals of the Mobilitics project are both to study the situation and trend, but also to make mobile terminal users aware of the situation, and to provide tools that may help them to better control the personnal information flow of their terminal.

## 6.3. Formal and legal issues of privacy

**Participants:** Thibaud Antignac, Denis Butin, Daniel Le Métayer.

- **Verification of privacy properties** The increasing official use of security protocols for electronic voting deepens the need for their trustworthiness, hence for their formal verification. The impossibility of linking a voter to her vote, often called voter privacy or ballot secrecy, is the core property of many such protocols. Most existing work relies on equivalence statements in cryptographic extensions of process calculi. We have proposed the first theorem-proving based verification of voter privacy which overcomes some of the limitations inherent to process calculi-based analysis [36]. Unlinkability between two pieces of information is specified as an extension to the Inductive Method for security protocol verification in Isabelle/HOL. New message operators for association extraction and synthesis are defined. Proving voter privacy demanded substantial effort and provided novel insights into both electronic voting protocols themselves and the analysed security goals. The central proof elements have been shown to be reusable for different protocols with minimal interaction.
- **Privacy by design** The privacy by design approach is often praised by lawyers as well as computer scientists as an essential step towards a better privacy protection. The general philosophy of privacy by design is that privacy should not be treated as an afterthought but rather as a first-class requirement during the design of a system. The approach has been applied in different areas such as smart metering, electronic traffic pricing, ubiquitous computing or location based services. More generally, it is possible to identify a number of core principles that are widely accepted and can form a basis for privacy by design. For example, the Organization for Economic Co-operation and Development (OECD) has put forward principles such as the consent, limitation of use, data quality, security and accountability. One must admit however that the take-up of privacy by design in the industry is still rather limited. This situation is partly due to legal and economic reasons: as long as the law does not impose binding commitments, ICT providers and data collectors do not have sufficient incentives to invest into privacy by design. The situation on the legal side might change in Europe though because the regulation proposed by the European Commission in January 2012 (to replace the European Directive 95/46/EC) includes binding commitments on privacy by design.

  But the reasons for the lack of adoption of privacy by design are not only legal and economic: even though computer scientists have devised a wide range of privacy enhancing tools, no general methodology is available to integrate them in a consistent way to meet a set of privacy requirements. The next challenge in this area is thus to go beyond individual cases and to establish sound foundations and methodologies for privacy by design. As a first step in this direction, we have focused on the data minimization principle which stipulates that the collection should be limited to the pieces of data strictly necessary for the purpose, and we have proposed a framework to reason about the choices of architecture and their impact in terms of privacy [53]. The first strategic choices are the allocation of the computation tasks to the nodes of the architecture and the types of communications between the nodes. For example, data can be encrypted or hashed, either to protect their confidentiality or to provide guarantees with respect to their correctness or origin. The main benefit of a centralized architecture for the "central" actor is that he can trust the result because he keeps full control over its computation. However, the loss of control by a single actor in decentralized architectures can be offset by extra requirements ensuring that errors (or frauds) can be detected *a posteriori*. In order to help the designer grasp the combination of possible options, our framework provides means to express the parameters to be taken into account (the service to be performed, the actors involved, their respective requirements, etc.) and an inference system to derive properties such as the possibility for an actor to detect potential errors (or frauds) in the computation of a variable. This inference system can be used in the design phase to check if an architecture meets the requirements of the parties or to point out conflicting requirements.
- **Privacy and discrimination**

Actually, the interactions between personal data protection, privacy and protection against discriminations are increasingly numerous and complex. For example, there is no doubt that misuses of personal data can adversely affect privacy and self-development (for example, resulting in the unwanted disclosure of personal data to third parties, in identity theft, or harassment through email or phone calls), or lead to a loss of choices or opportunities (for example, enabling a recruiter to obtain information over the internet about political opinions or religious beliefs of a candidate and to use this information against him). It could even be suggested that privacy breaches and discriminations based on data processing are probably the two most frequent and the most serious types of consequences of personal data breaches. We have studied these interactions from a multidisciplinary (legal and technical) perspective and argued that an extended application of the application of non-discrimination regulations could help strengthening data protection [52]. We have analysed and compared personal data protection, privacy and protection against discriminations considering both the types of data concerned and the *modus operandi* (*a priori* versus *a posteriori* controls, actors in charge of the control, etc.). From this comparison, we have drawn some conclusions with respect to their relative effectiveness and argued that *a posteriori* controls on the use of personal data should be strengthened and the victims of data misuse should get compensations which are significant enough to represent a deterrence for data controllers. We have also advocated the establishment of stronger connections between anti-discrimination and data protection laws, in particular to ensure that any data processing leading to unfair differences of treatments between individuals is prohibited and can be effectively punished [29].

## 6.4. Network measurement, modeling and understanding

**Participants:** Chadi Barakat, Arnaud Legout, Ashwin Rao, Walid Dabbous, Tessema Mindaye, Mohamed Ali Kaafar, Dong Wang, Vincent Roca, Ludovic Jacquin, Byungchul Park.

The main objective of our work in this domain is a better monitoring of the Internet and a better understanding of its traffic. We work on new measurement techniques that scale with the fast increase in Internet traffic and growth of its size. We propose solutions for a fast and accurate identification of Internet traffic based on packet size statistics and host profiles. Within the ANR CMON project, we work on monitoring the quality of the Internet access by end-to-end probes, and on the detection and troubleshooting of network problems by collaboration among end users.

Next, is a sketch of our main contributions in this area.

- **Checking Traffic Differentiation at the Internet Access**

  In the last few years, ISPs have been reported to discriminate against specific user traffic, especially if generated by bandwidth-hungry applications. The so-called network neutrality, advocating that an ISP should treat all incoming packets equally, has been a hot topic ever since. We propose Chkdiff, a novel method to detect network neutrality violations that takes a radically different approach from existing work: it aims at both application and differentiation technique agnosticism. We achieve this in three steps. Firstly, we perform measurements with the user's real traffic instead of using specific application traces. Secondly, we do not assume that discrimination takes place on any particular packet field, which requires us to preserve the integrity of all the traffic we intend to test. Thirdly, we detect differentiation by comparing the performance of a traffic flow against that of all other traffic flows from the same user, considered as a whole.

  Chkdiff is based on the following key ideas:
  Idea 1: **Use real user traffic**. We want to test the existence of traffic discrimination for the exact set of applications run by the end user. Hence, we only consider user-generated traffic.

Idea 2: **Leave user traffic unchanged, or almost**. All methods performing active measurements send probes made of real application packets and of packets that are similar, but slightly modified, so that they do not get discriminated along their path. This is quite an assumption, as we do not know exactly what ISPs do behind the scenes. In the extreme case, ISPs could even white-list traffic generated by differentiation detecting tools. It is therefore crucial to preserve as much of the original packets as possible, as well as their original per-flow order. We will see that the modifications introduced by our tool affect only the ordering of packets, their TTL value or their IP identification field.
Idea 3: **Baseline is the entire traffic performance**. Since we do not want to make any hypothesis in advance on what kind of mechanisms - if any - are deployed, we claim that the performance of each single non-differentiated flow should present the same behaviour as that of the rest of our traffic as a whole. Differentiated flows, on the other hand, should stand out when compared to all other flows grouped together, where a large fraction of non-differentiated flows should mitigate the impact of differentiated ones.

Chkdiff is currently the subject of a collaboration with I3S around the PhD thesis of Riccardo Ravaioli (funded by the Labex UCN@Sophia). A first description of the tool is presented in [63].

- **Lightweight Enhanced Monitoring for High-Speed Networks**

  Within the collaboration with Politecnico di Bari, we worked on LEMON, a lightweight enhanced monitoring algorithm based on packet sampling. This solution targets a pre-assigned accuracy on bitrate estimates, for each monitored flow at a router interface. To this end, LEMON takes into account some basic properties of the flows, which can be easily inferred from a sampled stream, and exploits them to dynamically adapt the monitoring time-window on a per-flow basis. Its effectiveness is tested using real packet traces. Experimental results show that LEMON is able to finely tune, in real-time, the monitoring window associated to each flow and its communication overhead can be kept low enough by choosing an appropriate aggregation policy in message exporting. Moreover, compared to a classic fixed-scale monitoring approach, it is able to better satisfy the accuracy requirements of bitrate estimates. Finally, LEMON incurs a low processing overhead, which can be easily sustained by currently deployed routers, such as a CISCO 12000 device. This work is currently under submission.

- **The Complete Picture of the Twitter Social Graph**

  In this work [49], we collected the entire Twitter social graph that consists of 537 million Twitter accounts connected by 23.95 billion links, and performed a preliminary analysis of the collected data. In order to collect the social graph, we implemented a distributed crawler on the PlanetLab infrastructure that collected all information in 4 months. Our preliminary analysis already revealed some interesting properties. Whereas there are 537 million Twitter accounts, only 268 million already sent at least one tweet and no more than 54 million have been recently active. In addition, 40% of the accounts are not followed by anybody and 25% do not follow anybody. Finally, we found that the Twitter policies, but also social conventions (like the followback convention) have a huge impact on the structure of the Twitter social graph.

- **Meddle: Middleboxes for Increased Transparency and Control of Mobile Traffic**

Mobile networks are the most popular, fastest growing and least understood systems in today's Internet ecosystem. Despite a large collection of privacy, policy and performance issues in mobile networks users and researchers are faced with few options to characterize and address them. In this work [62] we designed Meddle, a framework aimed at enhancing transparency in mobile networks and providing a platform that enables users (and researchers) control mobile traffic. In the mobile environment, users are forced to interact with a single operating system tied to their device, generally run closedsource apps that routinely violate user privacy, and subscribe to network providers that can (and do) transparently modify, block or otherwise interfere with network traffic. Researchers face a similar set of challenges for characterizing and experimenting with mobile systems. To characterize mobile traffic and design new protocols and services that are better tailored to the mobile environment, we would like a framework that allows us to intercept and potentially modify traffic generated by mobile devices as they move with users, regardless of the device, OS, wireless technology, or carrier. However, implementing this functionality is difficult on mobile devices because it requires warrantyvoiding techniques such as jail breaking to access and manipulate traffic at the network layer. Even when using such an approach, carriers may manipulate traffic once it leaves the mobile device, thus rendering some research impractical. Furthermore, researchers generally have no ability to deploy solutions and services such as prefetching and security filters, that should be implemented in the network. In this work, we designed Meddle, a framework that combines virtual private networks (VPNs) with middleboxes to provide an experimental platform that aligns the interests of users and researchers.

- **Mobile users' behavior modeling in Video on Demand systems and its implication on user privacy and caching strategies**

  In this project, we examine mobile users' behavior and their corresponding video viewing patterns from logs extracted from the servers of a large scale VoD system. We focus on the analysis of the main discrepancies that might exist when users access the VoD system catalog from WiFi or 3G connections. We also study factors that might impact mobile users' interests and video popularity. The users' behavior exhibits strong daily and weekly patterns, with mobile users' interests being surprisingly spread across almost all categories and video lengths, independently of the connection type. However, by examining the activity of users individually, we observed a concentration of interests and peculiar access patterns, which allows to classify the users and thus better predict their behavior. We also find the skewed video popularity distribution and demonstrate that the popularity of a video can be predicted using its very early popularity level. We then analyzed the sources of video viewing and found that even if search engines are the dominant sources for a majority of videos, they represent less than 10% (resp. 20%) of the sources for the highly popular videos in 3G (resp. WiFi) network. We also report that both the type of connection and the type of mobile device used have an impact on the viewing time and the source of viewing. Using our findings, we provide insights and recommendations that can be used to design intelligent mobile VoD systems and help in improving personalized services on these platforms. This work has been published in IMC 2012 [54].

- **Explicative models for Information Spreading on the web from a user profiling perspective**

  Microblog services offer a unique approach to online information sharing allowing microblog users to forward messages to others. We study the process of information diffusion in a microblog service developing Galton-Watson with Killing (GWK) model, which has many implications ranging from privacy protection to experiments validation and benchmarking. We describe an information propagation as a discrete GWK process based on Galton-Watson model which models the evolution of family names. Our model explains the interaction between the topology of the social graph and

the intrinsic interest of the message. We validate our models on dataset collected from Sina Weibo and Twitter microblogs. Sina Weibo is a Chinese microblog web service which reached over 100 million users as for January 2011. Our Sina Weibo dataset contains over 261 thousand tweets which have retweets and 2 million retweets from 500 thousand users. Twitter dataset contains over 1.1 million tweets which have retweets and 3.3 million retweets from 4.3 million users. The results of the validation show that our proposed GWK model fits the information diffusion of microblog service very well in terms of the number of message receivers. We show that our model can be used in generating tweets load and also analyze the relationships between parameters of our model and popularity of the diffused information. Our work is the first to give a systemic and comprehensive analysis for the information diffusion on microblog services, to be used in tweets-like load generators while still guaranteeing popularity distribution characteristics. Our paper illustrating this study will be presented in IEEE Infocom 2013 [69].

- **Tracking ICMP black holes at an Internet Scale**

  ICMP is a key protocol to exchange control and error messages over the Internet. An appropriate ICMP's processing throughout a path is therefore a key requirement both for troubleshooting operations (e.g. debugging routing problems) and for several functionalities (e.g. Path Maximum Transmission Unit Discovery, PMTUD). Unfortunately it is common to see ICMP malfunctions, thereby causing various levels of problems. In our study, we first introduce a taxonomy of the way routers process ICMP, which is of great help to understand for instance certain traceroute outputs. Secondly we introduce IBTrack, a tool that any user can use to automatically characterize ICMP issues within the Internet, without requiring any additional in-network assistance (e.g. there is no vantage point). Finally we validate our IBTrack tool with large scale experiments and we take advantage of this opportunity to provide some statistics on how ICMP is managed by Internet routers. This work has been presented in IEEE Globecom [51].

## 6.5. Experimental Environment for Future Internet Architecture

**Participants:** Walid Dabbous, Thierry Parmentelat, Fréderic Urbani, Daniel Camara, Alina Quereilhac, Shafqat Ur-Rehman, Mohamed Larabi, Thierry Turletti, Julien Tribino.

- **SFA Federation of experimental testbeds**

  We are now involved in the NOVI (E.U. STREP) project, the F-Lab (French A.N.R.) project, the FED4FIRE (E.U. IP) project and have the lead of the "Control Plane Extensions" WorkPackage of OpenLab (E.U. IP) project. Within these frameworks, as part of the co-development agreement between the Planète team and Princeton University, we have made a great deal of contributions into one of the most visible and renown implementations of the Testbed-Federation architecture known as SFA for Slice-based Federation Architecture. As a sequel of former activities we also keep a low-noise maintenance activity of the PlanetLab software, which has been running in particular on the PlanetLab global testbed since 2004, with an ad-hoc federated model in place between PlanetLab Central (hosted by Princeton University) and PlanetLab Europe (hosted at Inria) since 2007.

  During 2012, we have focused on the maturation of the SFA specifications and the SfaWrap codebase, with several objectives in mind. Firstly, we have contributed within the GENI (N.S.F.) project to the specifications of the Version 3 of the AM-API (Aggregate Manager API), which defines the primitives that a testbed management infrastructure has to provide in order to be SFA-compliant.

Secondly, knowing that our former SFA implementation was targeting PlanetLab testbeds only, we needed on the one hand, to make generic this SFA implementation, by completely redesign and refactor its codebase, and on the other hand, we needed to support all the resources allocation strategies supported by the testbeds, namely the allocation of both 'shared' and 'exclusive' resources. As a result of this redesign and development effort, out new SFA implementation is now disseminated and started to be known, under the name of SfaWrap, and we believe that it can be used as a production-grade alternative to quickly add SFA compatibility on top of many heterogenous testbed management frameworks.

Finally, in order to allow the community of networking researchers to execute cross-testbed experiments, involving heterogeneous resources, Planète team has been instrumental in federating a set of well-known testbeds through the SfaWrap, namely PlanetLab Europe, Senslab - developed in other Inria Project-teams -, FEDERICA, the outcome of another E.U.-funded project and more recently NITOS, an OMF-enabled wireless testbed. See [96] and [97] for more details.

- **Content Centric Networks Simulation**

  We worked this year on the extension of the DCE framework for ns-3 in order to run CCN implementation under the ns-3 simulator. DCE stands for Direct Code Execution, its goal is to execute unmodified C/C++ binaries under ns-3 network simulator. With this tool researchers and developpers can use the same code to do simulation and real experiments. DCE operation principle is to catch the standard systems calls done by the real application in the experiment and to emulate them within the ns-3 virtual network topology. Concerning CCN we use the PARC implementation named CCNx which is a well working open source software reference implementation of Content Centric Network protocol. As promised by DCE this integration of CCNx requires no modification of its code, it requires 'only' working on adding the system calls used by CCN that are not already supported by DCE. The advantage of this approach is that the integration work of CCN advanced DCE and will be useful in others completly different experiments. Another great advantage is that every evolution of the CCNx implementation is very easy to integrate, all what is needed is to compile the new source code. The next steps will be naturally to use DCE/ns-3 to evaluation CCN protocols in specific scenarii, to improve the coverage of systems calls supported by DCE, and to improve the DCE scheduler to be more realistic and to take into account CPU time spent in router queues. This work is done in the context of the ANR CONNECT project and is currently under submission.

- **ns-3 Module store**

  Bake is an integration tool which is used by software developers to automate the reproducible build of a number of projects which depend on each other and which might be developed, and hosted by unrelated parties. This software is being developed with the participation of the Planète group and is intended to be the automatic building tool adopted by the ns-3 project.

  The client version of Bake is already working and the Planète group had a significant participation in its development. The contributions were in the context the addition of new functionalities, bug fixing and in the development of the regression tests. We are now starting the development of the ns-3 modules repository, which is a web portal to store the meta-information of the available modules. In the present state we have already designed and implemented the portal data basis and the main interface. It is already possible to register new modules and browse among the already registered ones.

The web portal has to be finished, notably the part that will create the xml file that will be used to feed the bake's client. We also need to add new functionalities to the client part, to enable incremental build over partially deployed environments. As it is today, bake does not enable the user to add just one new module to an already deployed version of the ns-3 simulator. This work is done in the context of the ADT MobSim in collaboration with Hipercom and Swing Inria project-teams. For more details see the Bake web page http://planete.inria.fr/software/bake/index.html

- **The ns-3 consortium**

  We have founded last year a consortium between Inria and University of Washington. The goals of this consortium are to (1) provide a point of contact between industrial members and the ns-3 project, to enable them to provide suggestions and feedback about technical aspects, (2) guarantee maintenance of ns-3's core, organize public events in relation to ns-3, such as users' day and workshops and (3) provide a public face that is not directly a part of Inria or NSF by managing the http://www.nsnam.org web site.

- **Automated Deployment and Customization of Routing Overlays Across Heterogeneous Experimentation Platforms**

  During the last decades, many institutions and companies around the world have invested great effort into building new network experimentation platforms. These platforms range from simulators, to emulators and live testbeds, and provide very heterogeneous ways to access resources and to run experiments.

  Currently, a growing concern among platform owners is how to encourage researchers from different platform communities to take advantage of the resources they offer. However, one important aspect that needs to be overcome in order to appeal researchers to use as many experimentation platforms as necessary to best validate their results, is to decrease the inherent complexity to run experiments in different platforms. Even more so, to decrease the complexity of mixing resources from different platforms on a same experiment, to achieve the combination of resources best suited to the experiment needs.

  To address this concern, we developed the Network Experiment Programming Interface (NEPI) whose goal is to make easier the use of different experimentation platforms, and switch among them easily. The development of NEPI started in 2009 with the implementation of the core API, an address allocator, a routing table configurator, but also a prototype ns-3 backend driven by a simple graphical user interface based on QT. On 2010 we validated and evolved the core API with the addition of a new backend based on linux network namespace containers and stabilized the existing ns-3 backend.

  During 2011, we enhanced the design of NEPI and provided experiment validation, distributed experiment control, and failure recovery functionalities. In particular, we enforced separation between experiment design and execution stages, with off-line experiment validation. We also introduced a hierarchical distributed monitoring scheme to control experiment execution. We implemented a stateless message-based communication scheme, and added failure recovery mechanisms to improve robustness. Also on 2011, we started work on a prototype PlanetLab backend.

  Last year, we extended NEPI to provide automated deployment and customization of routing overlays using resources from heterogeneous experimentation platforms. The main contribution of this work is to enable researchers to easily integrate different resources, such as simulated, emulated or physical nodes, on a same experiment, using a network overlay, thus addressing one of the main concerns previously mentioned.

We started by adding support to easily build routing overlays on PlanetLab, and providing the ability to customize network traffic by adding user defined filters to packets traversing the overlay tunnels [48]. We then improved this work by adding the ability to include simulated nodes from the ns-3 backend and emulated nodes from the linux containers backend into a single overlay network. We demonstrated the use of NEPI to build adn control routing overlays which incorporate resources from different on the ns-3 2012 community workshop [74].

- **Content Centric Networks Live Experimentation**

  Realistic experimentation on top of Internet-like environments is key to evaluate the feasibility of world wide deployment of CCNx, and to assess the impact of existing Internet traffic conditions on CCN traffic. However, deploying live experiments on the Internet is a difficult and error prone task, specially when performed manually.

  To address this issue, during the last year, we extended NEPI, a framework for managing network experiments, to support easy design, and automated deployment and control, of CCNx experiments on the PlanetLab testbed. Among other features, NEPI now enables the deployment of user modified CCNx sources on arbitrary PlanetLab nodes, and the creation of tunnels to enable the use of multicast FIB entries between CCNx daemons over the Internet. By supporting easy CCNx experimentation on PlanetLab, NEPI can help to explore the co-existence of CCN and TCP/IP architecture.

  This work was presented as a poster and a demo at CCNxCon 2012, the CCNx http://www.ccnx.org/ community meeting [73]. The work had a very good reception and gained NEPI some new users.

  An online tutorial and demo were also made available at NEPI's web page http://nepi.inria.fr/wiki/nepi/CCNxOnPlanetLabEurope, for dissemination purposes.

- **Smooth-transition: a new methodology for dealing with various network experiment environments**

  The smooth-transition is a new methodology, which supports various network experiment environments covering from pure simulation through realistic emulation consistently. The reproducibility in experimental network research is getting important feature for iterative experiments in short-term and long-term period. The main idea of this concept is providing the reproducibility in a broader sense. So far, we had to implement different experiments by different environment, such as simulation, application-level emulation, and link-level emulation. Whereas the smooth-transition is able to keep the context of the experiments started from a pure simulation up to a realistic emulation gradually. That means the user does not need to waste time any more for learning and following a lot of documents and manuals from each different environment. Moreover, anyone can easily start to use the testbed and to develop inside (i.e. protocol stack). Because NS3 which is the most popular and powerful network simulator has been used in this concept as an experiment engine.

  The smooth-transition employees Network Experiment Programming Interface (NEPI) to conduct all functions, such as composing scenario, node deployment, experiment control, and resource management. The core of building this concept is NS3 which has Emulation (EMU) and Direct Code Execution (DCE) modules. EMU supports to use real network devices instead of NS3 MAC and PHY layer implementations. DCE is able to launch real application on top of NS3 protocol stacks. Furthermore, real Linux kernel (currently, net-next 2.6 is available) can replace NS3 Internet protocols by its advanced mode. This concept needs back-end system covering all experiment nodes. Control and Management Framework (OMF) plays an important role as a software framework to control and manage an wireless network testbed, and all messages are exchanged by Extensible Messaging and Presence Protocol (XMPP). Nitos scheduler has been adopted as a reservation system http://nitlab.inf.uth.gr/NITlab/index.php/scheduler. The user can reserve a time slot, nodes,

and wireless channels through its web page. In addition, SFA supports that the testbed is federated with other ones of outside.

The testbed provides PCAP files as a common outcome, and this file contains captured in and out packets. However, the file size is easily over gigabytes, then it makes a very long delay to process dozens of that files. To reduce the processing time efficiently, we are using an indexing scheme for fast collecting desired packets by filtering. In particular, this scheme is very useful to find packets occurred rarely, when an detailed analysis is required for an network event, such as retransmission, intrusion detection, and node association/disassociation. The indexing information is stored in a database file, and it does not need to be modified after making the file. The size of the file is very small compared with the PCAP file, so it provides fast packet filtering permanently, even after leaving the testbed. This work, post-processing of PCAP files, is in a collaboration with Diego Dujovne and Luciano Ahumada from the Universidad Diego Portales of Chili. Especially, YoungHwan Kim, a postdoc of the Planète group, has been currently dispatched for this collaboration for fourteen weeks (September 15 2012 $\sim$ January 26 2013) in Santiago, Chile.

- **The FIT experimental platform**

  We have started, since 2011, the procedure of building a new experimental platform at Sophia-Antipolis, in the context of the FIT Equipment of Excellence project. This platform has two main goals : the first one is to enable highly controllable experiments due to its anechoic environment. These experiments can be either hybrid-experiments (as NEPI will be deployed) or federated-experiments through several testbeds. The second goal is to make resource consuming experiments ( like CCNx ) possible due to some powerful servers that will be installed and connected to the PlanetLab testbed. During 2012, the specifications has been defined and the procedure will continue during the next year.

- **Network Simulations on a Grid**

  We studied an hybrid approach for the evaluation of networking protocols based on the ns-3 network simulator and a Grid testbed. We analyzed the performance of the approach using a simple use case. Our evaluation shows that the scalability of our approach is mainly limited by the processor speed and memory capacities of the simulation node. We showed that by exploiting the emulation capacity of ns-3, it is possible to map complex network scenarios on grid nodes. We also proposed a basic mapping algorithm to distribute a network scenario on several node [32].

# 7. Bilateral Contracts and Grants with Industry

## 7.1. Contracts with Industry

Industrial contract with Alcatel Lucent - Bell Labs (2008-2012):

The goal of this study is the use of AL-FEC techniques in broadcasting systems and in particular on the optimization of FEC strategies for wireless communications. Two persons are working in the context of this contract: Ferdaouss Mattoussi works on the design, analysis and optimization of a Generalized LDPC AL-FEC scheme, and Rodrigue Imad work focuses on Unequal Erasure Protection capabilities (UEP) and file bundle protection systems.

# 8. Partnerships and Cooperations

## 8.1. Regional Initiatives

PFT (2011-2014) : DGCIS funded project, in the context of the competitivity cluster SCS, whose aim is to provide to PACA region industrials wishing to develop or validate new products related to future mobile networks and services and M2M application, a networking infrastructure and tools helpful for development, test and validation of those products. Other partners : 3Roam, Audilog Groupe Ericsson, Ericsson, Eurecom, Inria, iQsim, MobiSmart, Newsteo, OneAccess, Orange Labs, Pôle SCS, ST Ericsson, Telecom Valley. Our contribution is centred around providing a test methodology and tools for wireless networks experimentation.

## 8.2. National Initiatives

ANR FIT (2011-2108): FIT (Future Internet of Things) aims to develop an experimental facility, a federated and competitive infrastructure with international visibility and a broad panel of customers. It will provide this facility with a set of complementary components that enable experimentation on innovative services for academic and industrial users. The project will give French Internet stakeholders a means to experiment on mobile wireless communications at the network and application layers thereby accelerating the design of advanced networking technologies for the Future Internet. FIT is one of 52 winning projects from the first wave of the French Ministry of Higher Education and Research's "Équipements d'Excellence" (Equipex) research grant programme. The project will benefit from a 5.8 million euro grant from the French government. Other partners are UPMC, IT, Strasbourg University and CNRS. See also http://fit-equipex.fr/.

ANR ARESA2 (2009-2012): The Planète team is involved in the ARESA2 project which aims at advancing the state of the art in Secure, Self-Organizing, Internet?Connected, Wireless Sensor and Actuator Networks (WSANs). These challenges are to be addressed in an energy-efficient way while sticking to memory-usage constraints. The partners are Inria, CEA-LETI, France Telecom R&D, Coronis Systems, LIG/Drakkar, Verimag and TELECOM Bretagne.

ANR pFlower (2010-2013): Parallel Flow Recognition with Multi-Core Processor. The main objective of this project is to take advantage of powerful parallelism of multi-thread, multi-core processors, to explore the parallel architecture of pipelined-based flow recognition, parallel signature matching algorithms. The project involves Inria (planete), Université de Savoie, and ICT/CAS (China).

Inria Mobilitics (2011-2012): as a joint national project with CNIL (the French national committee of Information freedom ). Platform for mobile devices privacy evaluation. This project strives to deploy an experimental mobile platform for studying and analyzing the weaknesses of current online (smartphone) applications and operating systems and the privacy implications for end-users. For instance, one of the objectives is to understand trends and patterns collected when they are aimed at obtaining general knowledge that does not pertain to any specific individual. Examples of such tasks include learning of commuting patterns, inference of recommendation rules, and creation of advertising segments.

Collaborative Action CAPRIS (2011-2014): the Collaborative Action on the Protection of Privacy Rights in the Information Society (CAPRIS), is an Inria national project, which goal is to tackle privacy-related challenges and provide solutions to enhance the privacy protection in the Information Society. His main tasks are the identification of existing and future threats to privacy, and the design of appropriate measures to assess and quantify privacy.

ANR CMON (2009-2012) : This project involves, in addition to Inria, Technicolor Paris Lab, LIP6, ENS and the Grenouille.com association. CMON stands for collaborative monitoring. It is an industrial research project that develops the technology needed to allow end-users to collaborate in order to identify the origin and cause of Internet service degradation. The main differentiating assumptions made in this project are that *(i)* ISPs do not cooperate together, and *(ii)* one cannot rely on any information they provide in order to diagnose service problems. Even more, CMON considers that these ISP will try to masquerade the user observations in order to make their service look better. The software designed in this project will be added to the toolbox currently provided by the Grenouille

architecture. The hope is that such a project will encourage ISPs to improve their quality of service and will contribute to improve customer satisfaction.

See also http://wiki.grenouille.com/index.php/CMON.

ANR F-Lab (2011-2013): ANR funded project on the federation of computation, storage and network resources, belonging to autonomous organizations operating heterogeneous testbeds (e.g. PlanetLab testbeds and Sensors testbeds). This includes defining terminology, establishing universal design principles, and identifying candidate federation strategies. Other partners : UPMC, A-LBLF and Thales.

ANR Connect (2011-2012): ANR funded project on content centric Networking architecture. The aim is to propose adequate naming, routing, cache management and transmission control schemes for CCN based networks. Our contribution is centered on network traffic characterization video streaming and on the integration of the CCNx code in the ns-3 simulator. Other partners: UPMC, Alcatel Lucent, Orange R&D, IT.

ANR SCATTER (2011-2012): ANR funded project on Scalable Naming in Information Centric Networks. The goal of this activity is to evaluate the scalability of state of the art naming schemes both from the name resolution and routing points of view. The four main approaches that will be considered are: Content Centric Networking (CCN), Publish-Subscribe Internet Routing Paradigm (PSIRP), Network of Information (NetInf) and Data-Oriented Network Architecture (DONA). Other French partners: UPMC. International KIC partner: SICS.

## 8.3. European Initiatives

### *8.3.1. FP7 Projects*

*8.3.1.1. NOVI*

Title: Networking innovations Over Virtualized Infrastructures

Type: COOPERATION (ICT)

Defi: CAPACITIES programme.

Instrument: Specific Targeted Research Project (STREP)

Duration: September 2010 - February 2013

Coordinator: NTUA (Greece)

Others partners: 13 european partners including GARR, ELTE, Cisco, etc.

See also: http://www.fp7-novi.eu/

Abstract: NOVI (Networking innovations Over Virtualized Infrastructures) research concentrates on efficient approaches to compose virtualized e-Infrastructures towards a holistic Future Internet (FI) cloud service. Resources belonging to various levels, i.e. networking, storage and processing are in principle managed by separate yet interworking providers. NOVI will concentrate on methods, information systems and algorithms that will enable users with composite isolated slices, baskets of resources and services provided by federated infrastructures.

*8.3.1.2. Fed4Fire*

Title: Federation for Future Internet Research and Experimentation

Type: COOPERATION (ICT)

Defi: FIRE programme.

Instrument: Integrating Project (IP)

Duration: October 2012 - October 2016

Coordinator: iMinds (Belgium)

Others partners: 17 european partners including iMinds, IT Innovation, UPMC, Fraunhofer, TUB, UEDIN, NICTA, etc.

See also: http://www.fed4fire.eu/

Abstract: Fed4FIRE will deliver open and easily accessible facilities to the FIRE experimentation communities, which focus on fixed and wireless infrastructures, services and applications, and combinations thereof. The project will develop a demand-driven common federation framework, based on an open architecture and specification. It will be widely adopted by facilities and promoted internationally. This framework will provide simple, efficient, and cost effective experimental processes built around experimenters' and facility owners' requirements. Insight into technical and socio-economic metrics, and how the introduction of new technologies into Future Internet facilities influences them, will be provided by harmonized and comprehensive measurement techniques. Tools and services supporting dynamic federated identities, access control, and SLA management will increase the trustworthiness of the federation and its facilities. A FIRE portal will offer brokering, user access management and measurements. Professional technical staff will offer first-line and second-line support to make the federation simple to use. The project will use open calls to support innovative experiments from academia and industry and to adapt additional experimentation facilities for compliance with Fed4FIRE specifications. A federation authority will be established to approve facilities and to promote desirable operational policies that simplify federation. A Federation Standardization Task Force will prepare for sustainable standardization beyond the end of the project. The adoption of the Fed4FIRE common federation framework by the FIRE facilities, the widespread usage by both academic and industrial experimenters, and the strong links with other national and international initiatives such as the FI-PPP, will pave the way to sustainability towards Horizon 2020.

*8.3.1.3. OPENLAB*

Title: OpenLab: extending FIRE testbeds and tools

Type: COOPERATION (ICT)

Defi: ICT 2011.1.6 Future Internet Research and Experimentation (FIRE)

Instrument: Integrated Project (IP)

Duration: September 2011 - January 2014

Coordinator: Université Pierre et Marie Curie (France)

Others partners: 18 European partners (including ETH Zurich, Fraunhofer, IBBT, TUB, UAM, etc.) and Nicta from Australia.

See also: http://www.ict-openlab.eu/

Abstract: OpenLab brings together the essential ingredients for an open, general purpose and sustainable large scale shared experimental facility, providing advances to the early and successful prototypes serving the demands of Future Internet Research and Experimentation.OpenLad partners are deploying the software and tools that allow these advanced testbeds to support a diverse set of applications and protocols in more efficient and flexible ways. OpenLab's contribution to a portfolio that includes: PlanetLab Europe (PLE), with its over 200 partner/user institutions across Europe; the NITOS and w-iLab.t wireless testbeds; two IMS telco testbeds that can connect to the public PSTN, to IP phone services, and can explore merged media distribution; an LTE cellular wireless testbed; the ETOMIC high precision network measurement testbed; the HEN emulation testbed; and the ns-3 simulation environment. Potential experiments that can be performed over the available infrastructure go beyond what can be tested on the current internet. OpenLab extends the facilities with advanced capabilities in the area of mobility, wireless, monitoring, domain interconnections and introduces new technologies such as OpenFlow. These enhancements are transparent to existing users of each facility. Finally, OpenLab will finance and work with users who propose innovative experiments using its technologies and testbeds, via the open call mechanism developed for FIRE facilities.

*8.3.1.4. FI-WARE*

Title: Future Internet Ware.

Type: COOPERATION (ICT).

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

Instrument: Integrated Project (IP).

Duration: May 2011 - April 2014.

Coordinator: Telefonica. (Spain)

Others partners: SAP (Germany), IBM (Israel, Switzerland), Thales Communications (France), Telecom Italia (Italy), France Telecom (France), Nokia Siemens Networks (Germany, Hungary, Finland), Deutsche Telekom (Germany), Technicolor (France), Ericsson (Sweden), Atos Origin (Spain), Ingeneria Informatica (Italy), Alcatel-Lucent (Italy, Germany), Siemens (Germany), Intel (Ireland), NEC (United Kingdom), Fraunhofer Institute (Germany), University of Madrid (Spain), University of Duisburg (Germany), University of Roma La Sapienza (Italy), University of Surrey (United Kingdom).

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

Abstract: The goal of the FI-WARE project is to advance the global competitiveness of the EU economy by introducing an innovative infrastructure for cost-effective creation and delivery of services, providing high QoS and security guarantees. FI-WARE is designed to meet the demands of key market stakeholders across many different sectors, e.g., healthcare, telecommunications, and environmental services. The project unites major European industrial actors in an unique effort never seen before. The key deliverables of FI-WARE will deliver an open architecture and implementation of a novel service infrastructure, building upon generic and reusable building blocks developed in earlier research projects. This infrastructure will support 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.

### *8.3.2. EIT KIC funded activities*

Our project team was involved in 2012 in **six activities** funded by the EIT ICT Labs KIC:

Title: **Fitting**, Future InterneT (of ThINGs) facility

Activity Number: 12340

Duration: 2011-2013

Coordinator: UPMC (France)

Others partners: Alcatel Lucent, Fraunhofer FOKUS, BME, IT, U. Paris XI.

Abstract: FITTING develops a testbed federation architecture that combines wireless and wired networks. Through FITTING, components and solutions developed in the projects OneLab2, PII and SensLAB are brought together to facilitate access. These components and devices complement each other – for instance SensLAB enhances the testbed federation by adding wireless sensors. FITTING addresses issues related to usability and accessibility of federated experimentation resources from multiple autonomous organizations. FITTING is a process of federating elements from various European and national initiatives into a global shared resource pool with a standardized interface to access them. Further, FITTING will adopt a user-driven (researchers, developers, students) approach with its running testbeds allowing experimentation with different technologies to meet the variety of needs of a broad customer base. The FITTING activity is mentioned as a “success story” by the EIT ICT Labs KIC [1]. In fact, after an initial funding in 2010, the french partners succeded to get the FIT Equipment of Excellence project accepted with a total budget of 5.8 MEuros to develop a testbed federation in France.

[1] See http://eit.europa.eu/kics1/stories-archiv/stories-single-view/article/fitting-from-eit-ict-labs-the-next-generation-testbeds.html

**Mobile Privacy**

This activity deals with privacy issues in mobile and geo-based systems.

**Smart-Space Privacy**

This activity deals with privacy issues in smart environments, with a particular issue on smart metering systems.

**Software-Defined Networking (SDN)**

The objective of this activity is to explore software-defined networking at different positions on the axis between basic flow-level processing (using OpenFlow for end-to-end flows) in controlled fixed networks and cooperation between mobile end nodes in the open wireless Internet (using opportunistic networking for resources communicated hop-by-hop).

**Information-centric networking (ICN) experimentation**

The goal of this activity is to define and implement an early validation environment for ICN proposals.

**Seamless P2P video streaming for the web**

In this activity, we will extend the current capabilities of the P2P network to distribute content to collaborators. We will analyze privacy concerns in this domain and propose design guidelines to mitigate them.

## 8.4. International Initiatives

### *8.4.1. Inria Associate Teams*

#### *8.4.1.1. COMMUNITY*

Title: Message delivery in heterogeneous networks

Inria principal investigator: Thierry Turletti

International Partner (Institution - Laboratory - Researcher):

University of California Santa Cruz (United States) - School of Engineering - Katia Obraczka

Duration: 2009 - 2014

See also: http://inrg.cse.ucsc.edu/community/

During the first three years of the COMMUNITY associate team, we have explored solutions to enable efficient delivery mechanisms for disruption-prone and heterogeneous networks (i.e. challenged networks). In particular, we have designed the MeDeHa framework along with the Henna naming scheme, which allow communication in infrastructure and infrastructure-less networks with varying degrees of connectivity. We have also proposed efficient routing strategies adapted to environment with episodic connectivity that take into account the utility of nodes to relay messages. The various solutions have been evaluated using both simulations and real experimentations in testbeds located at Inria and UCSC. These solutions have demonstrated good performance in challenged networks. However, the ossification of the Internet prevents the deployment of such solutions in large scale. We have decided to extend our collaboration in two research directions: (1) the exploration of the software-defined networking paradigm to facilitate the implementation and large scale deployment of new network architectures to infrastructure-less network environments; and (2) the design of innovative information-centric communication mechanisms adapted to challenged networks.

#### *8.4.1.2. SIMULBED*

Title: SIMULBED: Large-Scale Simulation Testbed for Realistic Evaluation of Network Protocols and Architectures

Inria principal investigator: Walid DABBOUS

International Partner (Institution - Laboratory - Researcher):

Keio University (Japan) - Shonan-Fujisawa Campus - Osamu Nakamura

Duration: 2012 - 2014

See also: http://planete.inria.fr/Simulbed

Simulators and experimental testbeds are two different approaches for the evaluation of network protocols and they provide a varying degree of repeatability, scalability, instrumentation and realism. Network simulators allow fine grained control of experimentation parameters, easy instrumentation and good scalability, but they usually lack realism. However, there is a growing need to conduct realistic experiments involving complex cross-layer interactions between many layers of the communication stack and this has led network researchers to evaluate network protocols on experimental testbeds.

The use of both simulators and testbeds to conduct experiments grants a better insight on the behavior of the evaluated network protocols and applications. In this project, we focus on the design of SIMULBED, an experimentation platform that aims to provide the best of both worlds. Our project builds on the following state-of-the-art tools and platforms: the open source ns-3 network simulator and the PlanetLab testbed. ns-3 is the first network simulator that includes a mechanism to execute directly within the simulator existing real-world Linux protocol implementations and applications. Furthermore, it can be used as a real-time emulator for mixed (simulation-experimentation) network scenarios. PlanetLab is the well-known international experimental testbed that supports the development and the evaluation of new network services. It is composed of nodes connected to the Internet across the world, and uses container-based virtualization to allow multiple experiments running independently on the same node while sharing its resources.

The overall objective of the project is to make available to networking research community, the SIMULBED platform that will: (1) allow to conduct easily mixed simulation-experimentation evaluation of networking protocols and (2) scale up the size of the PlanetLab experimental testbed, while maintaining a high degree of realism and increasing controllability and reproducibility. We will use the NEPI unified programming environment recently developed in the Planète project-team to help in simplifying the configuration, deployment and run of network scenarios on the platform.

*8.4.1.3. CLOUDY*

Title: Secure and Private Distributed Data Storage and Publication in the Future Internet

Inria principal investigator: ClaudeCastelluccia

International Partners (Institution - Laboratory - Researcher):

University of California Berkeley (United States) - Electrical Engineering and Computer Science Department - Edward Lee

University of California Irvine (United States) - Donald Bren School of Information and Computer Sciences - Gene Tsudik

Duration: 2012 - 2014

See also: http://planete.inrialpes.fr/cloudy-associated-team/

Cloud computing is a form of computing where general purpose clients (typically equipped with a web browser) are used to access resources and applications managed and stored on a remote server. Cloud applications are increasingly relied upon to provide basic services like e-mail clients, instant messaging and office applications. The customers of cloud applications benefit from outsourcing the management of their computing infrastructure to a third-party cloud provider. However, this places the customers in a situation of blind trust towards the cloud provider. The customer has to assume that the "cloud" always remains confidential, available, fault-tolerant, well managed, properly backed-up and protected from natural accidents as well as intentional attacks. An inherent reason for today's limitations of commercial cloud solutions is that end users cannot verify that servers in the cloud and the network in between are hosting and disseminating tasks and content without deleting, disclosing or modifying any content. This project seeks to develop novel technical solutions to allow customers to verify that cloud providers guarantee the confidentiality, availability and fault-tolerance of the stored data and infrastructure.

### *8.4.2. Participation In International Programs*

- CIRIC: Our project-team was involved in the definition of the topics for the Network and Telecom R&D line of the (the Communication and Information Research and Innovation Center - CIRIC), the Inria research and innovation centre in Chili. In this context, we will extend our collaboration with Universidad Diego Portales, Chile.

## 8.5. International Research Visitors

### *8.5.1. Visits of International Scientists*

Mostafa Ammar, Visiting Professor (one month in June 2012)

Subject: Investigating fundamenal properties of wireless and mobile networks

Institution: Georgia Institure of Technology (United States)

Paul de Hert, Visiting Professor (one month in June 2012)

Subject: Benefits and limitations of the legal notion of "reasonable expection of privacy"

Institution: Free University of Brussels (Belgium)

Katia Obraczka, Visiting Professor (one week in June 2012)

Subject: Communication in Heterogeneous Networks Prone to Episodic Connectivity

Institution: University of California at Santa Cruz (United States)

Marc Mendonca, Visiting PhD student (from Sep 2012 until Dec 2012)

Subject: Software-Defined Networking in Heterogeneous Networked Environments

Institution: University of California at Santa Cruz (United States)

Ilaria Cianci, Visiting PhD student (from Nov 2012 until Aug 2013)

Subject: Content Centric Networking

Institution: Politecnico di Bari, Italy

### *8.5.2. Visits to International teams*

Mohamed Ali Kaafar, spending a sabbatical at NICTA Australia in Sydney (since February 2012)

Subject: Online Privacy Enhancing Technologies: measuring the risks and designing countermeasures

Thierry Turletti, Visiting researcher to University of California at Santa Cruz (one week in February 2012)

Subject: Community Associated team

Thierry Turletti, Alina Quereilhac and Frederic Urbani, Visitors to NICT, Japan (one week in December 2012)

Subject: Simulbed Associated team

#### *8.5.2.1. Internships*

Riccardo Ravaioli (from Mar 2012 until Aug 2012)

Subject: Is the Internet neutral or content-aware? Handling the question by measurements

Institution: Master Ubinet - Sophia Antipolis

Tessema Mindaye (from Mar 2012 until Aug 2012)

Subject: Increasing the space of applications for statistical traffic classification methods

Institution: Master Ubinet - Sophia Antipolis

Francisco Santos (from Mar 2012 until Aug 2012)

Subject: Content management in mobile wireless networks

Institution: EPFL - Lausanne

Lucia Guevgeozian Odizzio (from May 2012 until Oct 2012)

Subject: Automatic IP address and routing table assignment for heterogeneous network topologies

Institution: Universitad de la Republica Oriental del Uruguay

Xuan-Nam Nguyen (from March 2012 until Aug 2012)

Subject: Software Defined Networking in Hybrid Networks

Institution: Université de Nice Sophia Antipolis (France)

Sumit BANSAL (from Feb 2012 until Jul 2012)

Subject: Attacks and Defenses for Secure Virtual Coordinate Systems

Institution: IIT Ropar (India)

# 9. Dissemination

## 9.1. Scientific Animation

Walid Dabbous served in the programme committees of NOMEN'2012, ICC'12 NGN and NoF'12. He is co-editor or a special issue of the PPNA journal on Experimental Evaluation of Peer-to-Peer Applications ([30]). He is member of the scientific council of the Inria Bell-Labs laboratory on Self Organizing Networks.

Claude Castelluccia served in the program committees of the following international conferences: ACM CCS 2012, ACM Wisec2012 and SESOC2012. He is the co-founder of the ACM WiSec (Wireless Security) conference.

Thierry Turletti Senior ACM and IEEE member, served in 2012 in the program committees of the following international conferences: 19th International Packet Video Workshop and 5th ACM Workshop on mobile Video Delivery (Movid). He is member of the Editorial Boards of the Journal of Mobile Communication, Computation and Information (WINET) published by Springer Science and of the Advances in Multimedia Journal published by Hindawi Publishing Corporation.

Chadi Barakat was the General Co-Chair of the ACM CoNEXT 2012 conference on emerging Networking EXperiments and Technologies that was held in Nice on Dec 10-13, 2012. In 2012, he served on the Technical Program Committee for the TMA 2013 workshop (Turin), the PAM 2013 conference (Hong-Kong), and the CNSM 2012 conference (Las Vegas). He is on the editorial board of the Elsevier Computer Networks journal. He is currently the scientific referee for international affairs at Inria Sophia Antipolis, and member of the Conseil d'Orientation Scientifique et Technologique (COST) at Inria within the working group of international affairs (COST-GTRI).

Vincent Roca is strongly involved at IETF and served as co-chair of the MSEC (Multicast Security) working group in 2010-2011. He is also member of the SecDir group (security directory) of the IETF. He was also member of the program committees of CFIP'09, SPACOMM'09, SPACOMM'10, the Cyber and Physical Security and Privacy symposium at IEEE SmartGridComm'11, CFIP'11, SPACOMM'11, SPACOMM'12.

Arnaud Legout was PC co-chair of the ICCCN 2009 conference track on P2P networking. He was also reviewer of journals (IEEE/ACM Transactions on Networking, IEEE/ACM Transactions on Computers, IEEE Network, Computer Communications, ACM SIGCOMM CCR), and conferences (IEEE Infocom, ACM Sigmetrics). He also served as an expert to the European Commission to evaluate EC funded projects.

Mohamed Ali Kaafar In 2012, he has been the program committee chair of ACM SIGMETRICS PADE workshop, and served in the program committees of the following international conferences: Internet Science 2013, Internet, ACM Sigcomm HotPlanet 2013, Interdisciplinarity & Innovation (In3 2013), Eurosys MPM 2013, IWAP2PT-2013, Colloque Jacques Cartier : Security, Inforensics and Cyber Criminality 2013, Eurosys MPM 2012, Sigmetrics PADE 2012, GridCom-2012, ICCSEA 2012, International Workshop on Trust and Privacy in Cyberspace (CyberTrust' 12), IWTMP2PS 2012. He is also member of the Editorial Board of the International Journal of peer-to-peer networks (IJP2P) and IEEE Transactions on Parallel and Distributed Systems TPDS and reviewer in SIGCOMM CCR, Computer Communications, IEEE letters of communications, Computer Networks. He was a panelist in IEEE CCW 2012 and an invited speaker in University of Concordia, UNSW and Polytechnic University of New York seminars.

Daniel Le Le Métayer served in the program committees of CPDP 2012, APF12, RISE12, FLACOS 2012 and APVP 2012. He organized a panel on privacy for location based services at CPDP 2012 and gave invited talks at the university of Chalmers, at the BDA Summer School, at IRILL (Paris), at CRIDS (Namur), at the ANR Privacy by Design Conference and at the conference organized by CNIL on "Privacy and Data Protection 2020".

## 9.2. Teaching - Supervision - Juries

### *9.2.1. Teaching*

Undergraduate course at IUT-2' (UPMF University), on network Communications, by Vincent Roca (24h).

Undergraduate course on Networking, by Walid Dabbous (36h), Ecole Polytechnique, Palaiseau, France.

Undergraduate course on Networks and Telecommunications, by Mohamed Ali Kaafar (40h), Ensimag Engineering school, France.

Undergraduate course at Polytech' Grenoble, on Wireless Communications, by Vincent Roca (12h).

Undergraduate course at IUT, Nice-Sophia Antipolis University, Local Aarea Networks by Chadi Barakat (28h), France.

Undergraduate course at IUP GMI Avignon on Peer-to-peer networks, by Arnaud Legout (38h), France.

Master Crypto and Security: course on Wireless Security by Claude Castelluccia (20h), Ensimag/University of Grenoble, France.

Master MOSIG: course on Wireless Security by Claude Castelluccia (15h), Ensimag/INPG, France.

Master FST : course on P2P networks: performance and security challenges by Mohamed Ali Kaafar (21h), Tunisia.

Master Phelma: course on Computer Networks by Mohamed Ali Kaafar (12h), INPG , France.

Master Ubinet: course on Evolving Internet - architectural challenges by Walid Dabbous and Chadi Barakat 42 hours, University of Nice-Sophia Antipolis, France.

Master CAR: course on Internet monitoring by Chadi Barakat, 3h, Telecom Paris Tech, France.

Master TSM: course on Voice over IP by Chadi Barakat, (7h),University of Nice-Sophia Antipolis, France.

Master Ubinet: course on Peer-to-peer networks, by Arnaud Legout (21), University of Nice-Sophia Antipolis.

Master SAFE: organization of a Teaching Unit on legal issues of security and privacy (30h) Daniel Le Le Métayer, University of Grenoble, France.

### *9.2.2. Supervision*

PhD : Eduardo Mazza defended his PhD titled “A formal framework for specifying and analyzing liabilities using log as digital evidence” on June 30th, at Grenoble University. His thesis was co-supervised by Daniel Le Le Métayer.

PhD : Amir Krifa defended his PhD titled “Towards better content dissemination applications for Disruption Tolerant Networks” on April 23rd 2012. His thesis was supervised by Chadi Barakat.

PhD: Shafqat Ur-Rehman defended his PhD titled “Benchmarking in Wireless Networks” on January 30th, 2012. His thesis was co-supervised by Thierry Turletti and Walid Dabbous.

PhD: Sana Ben Hamida defended her PhD on “Embedded System Security” on February 27th 2012. Her thesis was supervised by Claude Castelluccia.

PhD in progress : Lukasz Olejnik works on “Internet Tracking and Profiling” since 2011. His thesis is supervised by Claude Castelluccia.

PhD in progress : Min-Dung Tran works on “Privacy-Preserving Ad systems” since 2011. His thesis is co-supervised by Claude Castelluccia and Mohamed Ali Kaafar.

PhD in progress : Abdelberri Chaabane works on “Online Privacy in heterogeneous networks” since September 2010. His thesis is supervised by Mohamed Ali Kaafar.

PhD in progress : Thibaud Antignac works on “A formal framework for privacy by design” since September 2011. His thesis is supervised by Daniel Le Le Métayer.

PhD in progress: Riccardo Ravaioli works on “Active and Passive Inference of Network Neutrality” since October 2012. His thesis is co-supervised by Chadi Barakat.

PhD in progress : Dong Wang works on “Modeling social media and its impact on new digital ecnomy” since September 2011. His thesis is supervised by Mohamed Ali Kaafar.

PhD in progress: Xuan Nam Nguyen works on "Software Defined Networking in challenged environments", since October 2012. His thesis is co-supervised by Thierry Turletti and Walid Dabbous.

PhD in progress: Alina Quereilhac works on "Unified Evaluation environment of Networking Protocols for Simulators and Testbeds", since 2011. Her thesis is co-supervised by Walid Dabbous and Thierry Turletti.

PhD in progress: Ashwin Rao works on “Performance evaluation of communication networks”. His thesis is co-supervised by Arnaud Legout and Walid Dabbous.

PhD in progress: Ludovic Jacquin works on “High Bandwidth Secure Communications” since October 2009. His thesis is co-supervised by Vincent Roca and Jean-Louis Roch.

PhD in progress: Ferdaouss Mattoussi works on “Self-configuration and optimization of FEC over wireless protocol layers” since February 2010. Her work is co-supervised by Vincent Roca and Bessem Sayadi.

PhD in progress: Maksym Gabielkov works on “Propagation of data in social networks” since 2012. His work is supervised by Arnaud Legout.

PhD in progress: Wunan Gong works on “Security in content centric networks” since 2012. His work is supervised by Arnaud Legout.

PhD stopped: Anshuman Kalla stopped his PhD “Efficient transmission mechanisms for Information Centric Network Architectures” in june 2012 for personal reasons. His thesis was co-supervised by Thierry Turletti and Walid Dabbous.

# 10. Bibliography

## Major publications by the team in recent years

[1] C. CASTELLUCCIA, E. DE CRISTOFARO, D. PERITO. *Private Information Disclosure from Web Searches*, in "Proceedings of the 2010 Privacy Enhancing Technologies Symposium (PETS)", 2010.

[2] C. CASTELLUCCIA, A. FRANCILLON, C. SORIENTE, D. PERITO. *On the Difficulty of Software-Based Attestation of Embedded Devices*, in "CCS '09: Proceedings of the 16th ACM conference on Computer and communications security", 2009.

[3] C. CASTELLUCCIA, M. A. KAAFAR, P. MANILS, D. PERITO. *Geolocalization of Proxied Services and its Application to Fast-Flux Hidden Servers*, in "ACM/Usenix Internet Measurement Conference (IMC 2009)", Chicago, USA, ACM, November 2009.

[4] A. CHAABANE, G. ACS, M. A. KAAFAR. *You Are What You Like! Information leakage through users' Interests*, in "proceedings of the The Network & Distributed System Security Symposium (NDSS)", San Diego, February 2012.

[5] M. CUNCHE, V. SAVIN, V. ROCA. *Analysis of Quasi-Cyclic LDPC codes under ML decoding over the erasure channel*, in "IEEE International Symposium on Information Theory and its Applications (ISITA'10) (http://arxiv.org/abs/1004.5217)", April 2010.

[6] A. KRIFA, C. BARAKAT, T. SPYROPOULOS. *Message Drop and Scheduling in DTNs: Theory and Practice*, in "IEEE Transactions on Mobile Computing", 2012.

[7] I. LASSOUED, C. BARAKAT, K. AVRACHENKOV. *Network-wide monitoring through self-configuring adaptive system*, in "proceedings of IEEE INFOCOM", Shanghai, China, April 2011.

[8] S. LE BLOND, C. ZHANG, A. LEGOUT, K. ROSS, W. DABBOUS. *I Know Where You are and What You are Sharing: Exploiting P2P Communications to Invade Users' Privacy*, in "proceedings of ACM SIGCOM/USENIX IMC'11", Berlin, Germany, November 2011.

[9] A. LEGOUT, N. LIOGKAS, E. KOHLER, L. ZHANG. *Clustering and Sharing Incentives in BitTorrent Systems*, in "SIGMETRICS'07", San Diego, CA, USA, June 2007.

[10] T. LI, Q. NI, D. MALONE, D. LEIGHT, Y. XIAO, T. TURLETTI. *Aggregation with Fragment Retransmission for Very High-Speed WLANs*, in "IEEE/ACM Transactions on Networking Journal", 2009, vol. 17, n$^{o}$ 2.

[11] T. PAILA, R. WALSH, M. LUBY, V. ROCA, R. LEHTONEN. *FLUTE - File Delivery over Unidirectional Transport*, November 2012, IETF Request for Comments, RFC 6726 (Standards Track), http://hal.inria.fr/hal-00749951.

[12] D. PERITO, C. CASTELLUCCIA, M. A. KAAFAR, P. MANILS. *How Unique and Traceable are Usernames*, in "proceedings of the 11th Privacy Enhancing Technologies Symposium (PETS)", Waterloo, July 2011.

[13] A. RAO, Y.-S. LIM, C. BARAKAT, A. LEGOUT, D. TOWSLEY, W. DABBOUS. *Network Characteristics of Video Streaming Traffic*, in "proceedings of ACM CoNEXT'11", Tokyo, Japan, December 2011.

[14] K. B. RASMUSSEN, C. CASTELLUCCIA, T. HEYDT-BENJAMIN, S. CAPKUN. *Proximity-based Access Control for Implantable Medical Devices*, in "CCS '09: Proceedings of the 16th ACM conference on Computer and communications security", 2009.

[15] V. ROCA, C. NEUMANN, D. FURODET. *Low Density Parity Check (LDPC) Staircase and Triangle Forward Error Correction (FEC) Schemes*, June 2008, IETF Request for Comments, RFC 5170 (Standards Track/Proposed Standard).

[16] V. ROCA. *Simple Authentication Schemes for the Asynchronous Layered Coding (ALC) and NACK-Oriented Reliable Multicast (NORM) Protocols*, April 2012, IETF Request for Comments, RFC 6584 (Standards Track), http://hal.inria.fr/hal-00745908.

[17] D. SAUCEZ, L. IANNONE, O. BONAVENTURE, D. FARINACCI. *Designing a Deployable Internet: The Locator/Identifier Separation Protocol*, in "IEEE Internet Computing", 2012, vol. 16, p. 14-21, http://doi.ieeecomputersociety.org/10.1109/MIC.2012.98.

[18] K. SBAI, C. BARAKAT. *Experiences on enhancing data collection in large networks*, in "Computer Networks", May 2009, vol. 53, n° 7, p. 1073-1086.

[19] T. SPYROPOULOS, R. N. BIN RAIS, T. TURLETTI, K. OBRACZKA, A. VASILAKOS. *Routing for Disruption Tolerant Networks: Taxonomy and Design*, in "ACM/Springer Wireless Networks (WINET)", 2010, vol. 16, n° 8.

[20] T. SPYROPOULOS, T. TURLETTI, K. OBRACZKA. *Routing in Delay Tolerant Networks Comprising Heterogeneous Node Populations*, in "IEEE Transactions on Mobile Computing (TMC)", 2009, vol. 8, n° 8.

[21] M. WATSON, A. BEGEN, V. ROCA. *Forward Error Correction (FEC) Framework*, June 2011, IETF Request for Comments, RFC 6363 (Standards Track/Proposed Standard).

# Publications of the year

## Doctoral Dissertations and Habilitation Theses

[22] S. BEN HAMIDA. *Embedded System Security*, Université de Grenoble, February 2012.

[23] A. KRIFA. *Towards better content dissemination applications for Disruption Tolerant Networks*, Université de Nice Sophia Antipolis, April 2012.

[24] E. MAZZA. *A formal framework for specifying and analyzing liabilities using log as digital evidence*, Université de Grenoble, June 2012.

[25] S. UR-REHMAN. *Benchmarking in Wireless Networks*, Université de Nice Sophia Antipolis, January 2012.

## Articles in International Peer-Reviewed Journals

[26] A. APAVATJRUT, W. ZNAIDI, A. FRABOULET, C. GOURSAUD, K. JAFFRÈS-RUNSER, C. LAURADOUX, M. MINIER. *Energy Efficient Authentication Strategies for Network Coding*, in "Concurrency and Computation: Practice and Experience", July 2012, vol. 24, n° 10, p. 1086-1107 [*DOI :* 10.1002/CPE.1767], http://hal.inria.fr/hal-00644484.

[27] A. KRIFA, C. BARAKAT, T. SPYROPOULOS. *Message Drop and Scheduling in DTNs: Theory and Practice*, in "IEEE Transactions on Mobile Computing", 2012, vol. 11, n° 9.

[28] D. SAUCEZ, L. IANNONE, O. BONAVENTURE, D. FARINACCI. *Designing a Deployable Internet: The Locator/Identifier Separation Protocol*, in "IEEE Internet Computing", 2012, vol. 16, p. 14-21, http://doi.ieeecomputersociety.org/10.1109/MIC.2012.98.

### Articles in National Peer-Reviewed Journals

[29] J. LE CLAINCHE, D. LE MÉTAYER. *Vie privée et non discrimination: des protections complémentaires, une convergence nécessaire*, in "Revue Lamy Droit de l'Immatériel", 2013, to appear.

### Articles in Non Peer-Reviewed Journals

[30] R. CANONICO, C. CANALI, W. DABBOUS. *Experimental evaluation of peer-to-peer applications*, in "Peer-to-Peer Networking and Applications", 2012, Editorial paper, http://link.springer.com/article/10.1007/s12083-012-0177-z/fulltext.html.

[31] A. LEGOUT, W. DABBOUS. *Linking a Social Identity to an IP Address*, in "ERCIM News", 2012, n$^{o}$ 90.

### International Conferences with Proceedings

[32] A. ABIDI, S. GAMMAR, F. KAMOUN, W. DABBOUS, T. TURLETTI, A. LEGOUT. *Hybrid approach for experimental networking research*, in "13th International Conference on Distributed Computing and Networking (ICDCN)", Hong Kong, China, January 2012, http://www-sop.inria.fr/members/Thierry.Turletti/icdcn11.pdf.

[33] G. ACS, C. CASTELLUCCIA, R. CHEN. *Differentially Private Histogram Publishing through Lossy Compression*, in "International Conference Data Mining", Brussels, Belgique, 2012, http://hal.inria.fr/hal-00747821.

[34] K. AVRACHENKOV, P. GONCALVES, A. LEGOUT, M. SOKOL. *Classification of Content and Users in BitTorrent by Semi-Supervised Learning Methods*, in "Proc. of IEEE IWCMC'2012, TRAC Workshop", Limassol, Cyprus, IEEE, August 2012.

[35] A. BENFARAH, B. MISCOPEIN, C. LAURADOUX, J.-M. GORCE. *Towards Stronger Jamming Model: Application to TH-UWB Radio*, in "IEEE WCNC - Wireless Communications and Networking Conference", Paris, France, April 2012, http://hal.inria.fr/hal-00758577.

[36] D. BUTIN, D. GRAY, G. BELLA. *Towards Verifying Voter Privacy Through Unlinkability*, in "Proceedings of the International Symposium on Engineering Secure Software and Systems (ESSoS 2013)", Springer Verlag, 2013, to appear.

[37] C. CASTELLUCCIA, M. A. KAAFAR, M.-D. TRAN. *Betrayed by Your Ads!*, in "PETS- Privacy Enhancing Tools Symposium", Vigo, Espagne, July 2012, http://hal.inria.fr/hal-00747823.

[38] C. CASTELLUCCIA, D. PERITO, D. MARKUS. *Adaptive Password-Strength Meters from Markov Models*, in "19th Annual Network & Distributed System Security Symposium (NDSS)", San Diego, États-Unis, ISOC, February 2012, http://hal.inria.fr/hal-00747824.

[39] A. CHAABANE, G. ACS, M. A. KAAFAR. *You Are What You Like! Information Leakage Through Users' Interests*, in "Proc. Annual Network and Distributed System Security Symposium NDSS", 2012.

[40] A. CHAABANE, M. A. KAAFAR, R. BORELI. *Big friend is watching you: analyzing online social networks tracking capabilities*, in "Proceedings of the 2012 ACM SIGCOMM workshop on Workshop on online social networks", ACM, 2012, p. 7–12.

[41] R. CHEN, G. ACS, C. CASTELLUCCIA. *Differentially Private Sequential Data Publication via Variable-Length N-Grams*, in "ACM Computer and Communication Security (CCS)", Raleigh, États-Unis, ACM, October 2012, http://hal.inria.fr/hal-00747830.

[42] T. CHEN, M. A. KAAFAR, A. FRIEDMAN, R. BORELI. *Is more always merrier?: a deep dive into online social footprints*, in "Proceedings of the 2012 ACM SIGCOMM workshop on Workshop on online social networks", ACM, 2012, p. 67–72.

[43] N. CHENG, P. MOHAPATRA, M. CUNCHE, M. A. KAAFAR, R. BORELI, V. SRIKANTH. *Inferring User Relationship from Hidden Information in WLANs*, in "MILCOM - IEEE Military Communications Conference - 2012", Orlando, États-Unis, 2012, http://hal.inria.fr/hal-00747850.

[44] F. CORAS, D. SAUCEZ, L. JAKAB, A. CABELLOS-APARICIO, J. DOMINGO-PASCUAL. *Implementing a BGP-Free ISP Core with LISP*, in "Globecom 2012", 2012.

[45] M. CUNCHE, M. A. KAAFAR, R. BORELI. *I know who you will meet this evening! Linking wireless devices using Wi-Fi probe requests*, in "World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a", IEEE, 2012, p. 1–9.

[46] M. CUNCHE, M. A. KAAFAR, T. CHEN, R. BORELI, A. MAHANTI. *Why are they hiding ? Study of an Anonymous File Sharing System*, in "ESTEL-SEC - Security and Privacy Special Track of IEEE-AESS Conference in Europe about Space and Satellite Communications - 2012", Rome, Italie, October 2012, http://hal.inria.fr/hal-00747833.

[47] M. DARDAILLON, C. LAURADOUX, T. RISSET. *Hardware Implementation of the GPS authentication*, in "ReConFig - International Conference on ReConFigurable Computing and FPGAs", Cancun, Mexique, December 2012, http://hal.inria.fr/hal-00737003.

[48] C. FREIRE, A. QUEREILHAC, T. TURLETTI, W. DABBOUS. *Automated deployment and customization of routing overlays on PlanetLab*, in "ICSC TridentCom Conference 2012", Thessaloniki, Greece, June 2012, http://planete.inria.fr/Simulbed/Tridentcom12nepi.pdf.

[49] M. GABIELKOV, A. LEGOUT. *The Complete Picture of the Twitter Social Graph*, in "Proc. of ACM CoNext 2012", Nice, France, December 2012.

[50] S. HAMIDA TMAR-BEN, P. JEAN-BENOIT, B. DENIS, B. UGUEN, C. CASTELLUCCIA. *On the security of UWB secret key generation methods against deterministic channel prediction attacks*, in "Vehicular Technology Conference (VTC)", Quebec, Canada, IEEE, September 2012, http://hal.inria.fr/hal-00747839.

[51] L. JACQUIN, V. ROCA, M. A. KAAFAR, F. SCHULER, J.-L. ROCH. *IBTrack: an ICMP black holes tracker*, in "Proceedings of IEEE Globecom", IEEE, 2012.

[52] D. LE MÉTAYER, J. LE CLAINCHE. *From the protection of data to the protection of individuals: extending the application of non discrimination principles*, in "European Data Protection: In Good Health ?", S. GUTWIRTH, Y. POULLET, P. DE HERT (editors), Springer Verlag, 2012, p. 315-330.

[53] D. LE MÉTAYER. *Privacy by design: a formal framework for the analysis of architectural choices*, in "Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY 2013)", IEEE, 2013, to appear.

[54] Z. LI, J. LIN, M. AKODJENOU, G. XIE, M. KAAFAR, Y. JIN, G. PENG. *Watching Videos from Everywhere: a Study of the PPTV Mobile VoD System*, in "Proceedings of the ACM SIGCOMM conference on Internet measurement conference", ACM, 2012.

[55] F. MATTOUSSI, V. ROCA, B. SAYADI. *Complexity Comparison Of The Use Of Vandermonde Versus Hankel Matrices To Build Systematic MDS Reed-Solomon Codes*, in "SPAWC 2012 - 13th IEEE Internation Workshop on Signal Processing Advances in Wireless Communications", CESME, Turkey, June 2012, http://hal.inria.fr/hal-00719314.

[56] F. MATTOUSSI, V. ROCA, B. SAYADI. *Design of Small Rate, Close to Ideal, GLDPC-Staircase AL-FEC Codes for the Erasure Channel*, in "IEEE Globecom 2012", Anaheim, United States, Dr. Hossein Eslambolchi (organizing committee general chair), Dec 2012, http://hal.inria.fr/hal-00736071.

[57] F. MATTOUSSI, V. SAVIN, V. ROCA, B. SAYADI. *Optimization With Exit Functions Of GLDPC-Staircase Codes For The BEC*, in "SPAWC 2012 - 13th IEEE Internation Workshop on Signal Processing Advances in Wireless Communications", CESME, Turkey, June 2012, http://hal.inria.fr/hal-00719321.

[58] M. MENDONCA, K. OBRACZKA, T. TURLETTI. *The Case for Software-Defined Networking in Heterogeneous Networked Environments*, in "ACM CoNEXT Student Workshop 2012", Nice, France, December 2012, Poster, http://inrg.cse.ucsc.edu/community/Publications?action=AttachFile&do=get&target=hsdn-mini.pdf.

[59] X. MISSERI, J.-L. ROUGIER, D. SAUCEZ. *Internet routing diversity for stub networks with a Map-and-Encap scheme*, in "IEEE ICC 2012", 2012.

[60] L. OLEJNIK, C. CASTELLUCCIA, A. JANC. *Why Johnny Can't Browse in Peace: On the Uniqueness of Web Browsing History Patterns*, in "5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2012)", Vigo, Espagne, July 2012, http://hal.inria.fr/hal-00747841.

[61] A. QUEREILHAC, T. TURLETTI, W. DABBOUS. *A Multi-Platform Event-Driven Controller for Network Experiments*, in "ACM CoNEXT Student Workshop 2012", Nice, France, December 2012, Poster, http://conferences.sigcomm.org/co-next/2012/eproceedings/student/p33.pdf.

[62] A. RAO, D. CHOFFNES, J. SHERRY, A. LEGOUT, A. KRISHNAMURTHY, W. DABBOUS. *Meddle: Middleboxes for Increased Transparency and Control of Mobile Traffic*, in "Proc. of ACM CoNext 2012", Nice, France, December 2012.

[63] R. RAVAIOLI, C. BARAKAT, G. URVOY-KELLER. *Chkdiff: Checking Traffic Differentiation at Internet Access*, in "ACM CoNEXT Student Workshop", Nice, France, December 2012.

[64] A. ROUMY, V. ROCA, B. SAYADI. *Memory Consumption Analysis for the GOE and PET Unequal Erasure Protection Schemes*, in "IEEE International Conference on Communications", Ottawa, Canada, February 2012, http://hal.inria.fr/hal-00668826.

[65] D. SAUCEZ, B. DONNET. *On the dynamics of locators in LISP*, in "Proceedings of the 11th international IFIP TC 6 conference on Networking - Volume Part I", Berlin, Heidelberg, IFIP'12, Springer-Verlag, 2012, p. 385–396, http://dx.doi.org/10.1007/978-3-642-30045-5_29.

[66] D. SAUCEZ, W. HADDAD. *Network in the Cloud: a Map-and-Encap Approach*, in "IEEE CloudNet 2012", November 2012.

[67] D. SAUCEZ, J. KIM, L. IANNONE, O. BONAVENTURE, C. FILSFILS. *A local approach to fast failure recovery of LISP ingress tunnel routers*, in "Proceedings of the 11th international IFIP TC 6 conference on Networking - Volume Part I", Berlin, Heidelberg, IFIP'12, Springer-Verlag, 2012, p. 397–408, http://dx.doi.org/10.1007/978-3-642-30045-5_30.

[68] C. TESTA, D. ROSSI, A. RAO, A. LEGOUT. *Experimental Assessment of BitTorrent Completion Time in Heterogeneous TCP/uTP swarms*, in "Proc. of Traffic Monitoring and Analysis (TMA) Workshop", Vienna, Austria, March 2012.

[69] G. WANG, H. PARK, G. XIE, S. MOON, M. KAAFAR, K. SALAMATIAN. *A Genealogy of Information Spreading on Microblogs: a Galton-Watson-based Explicative Model*, in "Proceedings of IEEE Infocom", IEEE, 2013.

[70] Y. WANG, G. XIE, M. KAAFAR. *FPC: A self-organized greedy routing in scale-free networks*, in "Computers and Communications (ISCC), 2012 IEEE Symposium on", IEEE, 2012, p. 000102–000107.

### Conferences without Proceedings

[71] D. CAMARA, F. URBANI, M. LACAGE, T. TURLETTI, W. DABBOUS. *Simulation Platform for Content Centric Networks Protocols Development*, in "CCNx Workshop 2012", Sophia Antipolis, France, September 2012, http://planete.inria.fr/Simulbed/ns3-ccnxcon12.pdf.

[72] A. QUEREILHAC, C. FREIRE, T. TURLETTI, W. DABBOUS. *Controllable packet prioritization on PlanetLab using NEPI*, in "Demo at ICSC TridentCom 2012", Thessaloniki, Greece, June 2012.

[73] A. QUEREILHAC, A. KALLA, T. TURLETTI, W. DABBOUS. *Easy CCNx experimentation on PlanetLab*, in "Demo at CCNx Workshop 2012", Sophia Antipolis, France, September 2012, http://planete.inria.fr/Simulbed/nepi-ccnxcon12.pdf.

[74] A. QUEREILHAC, T. TURLETTI, W. DABBOUS. *Managing heterogeneous ns-3 experiments with NEPI*, in "Poster at WNS3 Workshop 2012", Desenzano, Italy, March 2012, http://www.nsnam.org/wp-content/uploads/2011/10/nepiWNS3Poster_1200.pdf.

[75] D. SAUCEZ, L. A. GRIECO, C. BARAKAT. *AIMD and CCN: past and novel acronyms working together in the Future Internet*, in "ACM CoNEXT Capacity Sharing Workshop 2012 (CSWS12)", 2012.

### Research Reports

[76] F. DE MENESES NEVES RAMOS DOS SANTOS, C. BARAKAT, T. SPYROPOULOS, T. TURLETTI. *Content Management in Mobile Wireless Networks*, Inria, 2012, 54, http://hal.inria.fr/hal-00742734.

[77] F. GOICHON, C. LAURADOUX, G. SALAGNAC, T. VUILLEMIN. *Entropy transfers in the Linux Random Number Generator*, Inria, September 2012, n$^{o}$ RR-8060, 26, http://hal.inria.fr/hal-00738638.

[78] T. PAILA, R. WALSH, M. LUBY, V. ROCA, R. LEHTONEN. *FLUTE - File Delivery over Unidirectional Transport (revised)*, June 2012, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-16.txt>.

[79] T. PAILA, R. WALSH, M. LUBY, V. ROCA, R. LEHTONEN. *FLUTE - File Delivery over Unidirectional Transport (revised)*, June 2012, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-15.txt>.

[80] T. PAILA, R. WALSH, M. LUBY, V. ROCA, R. LEHTONEN. *FLUTE - File Delivery over Unidirectional Transport (revised)*, March 2012, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-14.txt>.

[81] T. PAILA, R. WALSH, M. LUBY, V. ROCA, R. LEHTONEN. *FLUTE - File Delivery over Unidirectional Transport (revised)*, January 2012, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-13.txt>.

[82] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, November 2012, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-newfcast-07.txt>.

[83] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, October 2012, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-newfcast-06.txt>.

[84] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, October 2012, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-newfcast-05.txt>.

[85] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Simple Reed-Solomon Forward Error Correction (FEC) Scheme for FECFRAME*, November 2012, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-simple-rs-05>.

[86] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Simple Reed-Solomon Forward Error Correction (FEC) Scheme for FECFRAME*, October 2012, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-simple-rs-04>.

[87] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Simple Reed-Solomon Forward Error Correction (FEC) Scheme for FECFRAME*, March 2012, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-simple-rs-03>.

[88] V. ROCA, M. CUNCHE, J. LACAN. *Simple LDPC-Staircase Forward Error Correction (FEC) Scheme for FECFRAME*, October 2012, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-ldpc-04.txt>.

[89] V. ROCA, M. CUNCHE, J. LACAN. *Simple LDPC-Staircase Forward Error Correction (FEC) Scheme for FECFRAME*, October 2012, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-ldpc-03.txt>.

[90] V. ROCA, M. CUNCHE, J. LACAN. *Simple LDPC-Staircase Forward Error Correction (FEC) Scheme for FECFRAME*, March 2012, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-ldpc-02.txt>.

[91] V. ROCA, A. ROUMY, B. SAYADI. *The Generalized Object Encoding (GOE) Approach for the Forward Erasure Correction (FEC) Protection of Objects and its Application to Reed- Solomon Codes over GF(2x)*, March 2012, IETF RMT Working Group, Work in Progress: <draft-roca-rmt-goe-fec-01.txt>.

[92] V. ROCA, A. ROUMY, B. SAYADI. *The Generalized Object Encoding (GOE) LDPC-Staircase FEC Scheme*, July 2012, IETF RMT Working Group, Work in Progress: <draft-roca-rmt-goe-ldpc-01.txt>.

[93] V. ROCA, A. ROUMY, B. SAYADI. *The Need for Extended Forward Erasure Correction (FEC) schemes: Problem Position*, Inria, July 2012, http://hal.inria.fr/hal-00752510.

## Other Publications

[94] X.-N. NGUYEN. *Software Defined Networking in Wireless Mesh Network*, Université de Nice Sophia Antipolis, France, August 2012, UBINET MSc Thesis, http://inrg.cse.ucsc.edu/community/Publications?action=AttachFile&do=get&target=nam-ms.pdf.

[95] T. PAILA, R. WALSH, M. LUBY, V. ROCA, R. LEHTONEN. *FLUTE - File Delivery over Unidirectional Transport*, November 2012, IETF Request for Comments, RFC 6726 (Standards Track), http://hal.inria.fr/hal-00749951.

[96] T. PARMENTELAT, J. AUGÉ, S. AVAKIAN, L. BARON, M. LARABI, N. TURRO. *Federation : implementation report*, October 2012, ANR F-LAB project deliverable D1.2, http://git.f-lab.fr/?p=d12.git;a=blob;f=d12.pdf;h=7ec59cfbc214e4a6a143d0f286d7c64671fc01e4;hb=HEAD.

[97] T. PARMENTELAT, A. WILLNER, C. TRANORIS, T. RAKOTOARIVELO, J. AUGÉ. *Control plane extension*, September 2012, FP7 OpenLab project deliverable D1.1, https://git.ict-openlab.eu/?p=deliverable1.1.git;a=blob_plain;f=d11.pdf;hb=HEAD.

[98] V. ROCA. *Simple Authentication Schemes for the Asynchronous Layered Coding (ALC) and NACK-Oriented Reliable Multicast (NORM) Protocols*, April 2012, IETF Request for Comments, RFC 6584 (Standards Track), http://hal.inria.fr/hal-00745908.

[99] D. SAUCEZ, C. BARAKAT, T. TURLETTI. *Leveraging Information Centric Networking in Over-The-Top Services*, February 2012, Under submission Journal of Network and Systems Management, http://hal.inria.fr/hal-00684458.

[100] D. SAUCEZ, A. KALLA, C. BARAKAT, T. TURLETTI. *Minimizing Bandwidth on Peering Links with Deflection in Named Data Networking*, March 2012, unpublished note, http://hal.inria.fr/hal-00684453.

[101] C. THIENNOT, C. SEYRAT, V. ROCA, J. DETCHART. *Proposal for a Candidate for EMM-EFEC Work Item*, May 2012, Document S4-120731, 3GPP TSG-SA4 meeting 69, Erlangen, Germany.

[102] C. THIENNOT, C. SEYRAT, V. ROCA, J. DETCHART. *RS+LDPC EMM-EFEC contribution*, August 2012, Document S4-121024, 3GPP TSG-SA4 meeting 70, Chicago, USA.

[103] C. THIENNOT, C. SEYRAT, V. ROCA, J. LACAN, J. DETCHART. *RS+LDPC EMM-EFEC contribution - update*, November 2012, Document S4-121471, 3GPP TSG-SA4 meeting 71, Bratislava, SLOVAKIA.