Activity Report 2011

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

1. Members

Research Scientists

Walid Dabbous [Team Leader, Senior Researcher, Inria, HdR]
Claude Castelluccia [Senior Researcher, Inria, HdR]
Thierry Turletti [Senior Researcher, Inria, HdR]
Chadi Barakat [Junior Researcher, Inria, HdR]
Mohamed Ali Kaafar [Junior Researcher, Inria]
Arnaud Legout [Junior Researcher, Inria]
Vincent Roca [Junior Researcher, Inria]

Technical Staff

Jonathan Detchart [Associate Engineer ADT until November 2011 and Expert Engineer since December 2011]
Amir Krifa [Expert Engineer until July 2011]
Baris Metin [Expert Engineer, until January 2011]
Thierry Parmentelat [Dream Engineer]
Alina Quereilhac [Associate Engineer then Expert Engineer and PhD student]
Saghar Estehghari [Associate Engineer, until November 2011]
Fabrice Schuler [Expert Engineer]
Daniel Camara [Experienced Engineer since October 2011]
Fréderic Urbani [Expert Engineer since April 2011]
Julien Tribino [Associate Engineer since December 2011]

PhD Students

Sana Ben Hamida [Funding CEA LETI]
Abdelberi Chaabane [Funding ANR ARESA2 contract]
Mohamad Jaber [Funding MESR Scholarship & ATER]
Ludovic Jacquin [Minalogic Inria grant]
Imed Lassoued [Funding ECODE project until August 2011]
Stevens Le Blond [Funding Inria CORDIS Scholarship & OneLab2 contract until April 2011]
Ferdaouss Mattoussi [Funding ADR Alcatel Lucent contract]
Daniele Perito [Funding WSN4CIP IST project]
Rao Naveed Bin Rais [Funding Pakistanian Scholarship]
Ashwin Rao [Funding OneLab2 and Connect projects]
Shafqat Ur-Rehman [Funding F-Lab project]
Anshuman Kalla [Funding FRM, since December 2011]
Dong Wang [Funding ANR PFlower project, since September 2011]
Min-Dung Tran [Funding Allocation of Ministry of national Education since September 2011]

Post-Doctoral Fellows

Gergely Acs [Funding Inria CORDIS]
Roberto Cascella [Funding ANR C'MON]
Damien Saucez [Funding Inria scholarship]

Visiting Scientists

Luigi Alfredo Grieco [Visiting Professor from University of Bari, one week in December 2011]
Katia Obraczka [Visiting Professor from UCSC, one week in January 2011 and one week in November 2011]
Marc Mendonca [Visiting PhD student from UCSC, from September 2011 to December 2011]

Administrative Assistants

Anais Cassino [Sophia]
Helen Pouchot [Grenoble]

Others

Anasthesia Fedane [University of Grenoble intern, from February to July 2011]
Min-Dung Tran [University of Grenoble intern, from February to July 2011]
Lecat William [Ecole Polytechnique intern, from April to June 2011]
Manu Sekar [International Programme in Wireless Networks and Security, from Feb. 2011 to July 2011]
Mauricio Jost [Ubinet Master program Intern, from April to August 2011]
Hervé Falciani [Ubinet Master program Intern, from March to August 2011]
Sandun Wijayarathne [Ubinet Master program Intern, from April to August 2011]
Claudio Freire [University of Buenos Aires Intern, from April to August 2011]
Blerina Lika [University of Athens Intern, from June to July 2011]
Ana Nika [University of Athens Intern, from March to July 2011]

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

- Our work on "tracking Skype users mobility" received a lot of media attention this year (tens of articles in Le Monde, The New York Times, Slashdot, The Register, and more generally in international technical and general audience press...). This work has been published in IMC 2011[46].
- Our work on "usernames uniqueness and traceability" has been published in PETS 2011 [47], one of the most prestigious conference in the area of Computer Privacy, and has been awarded the Andreas Pfitzmann award for the best contribution. It also received a lot of media attention.
- Our LDPC-Staircase codes have been included this year as the primary AL-FEC (Application Layer Forward Erasure Correction code) solution for ISDB-Tmm (Integrated Services Digital Broadcasting, Terrestrial Mobile Multimedia), a Japanese standard for digital television (DTV) and digital radio. The commercial launch of ISDB-Tmm will happen in mid 2012. This success has been made possible, on the one hand, by major efforts in terms of standardization within IETF and on the other hand, by our efforts in terms of design and evaluation of two efficient software codecs of LDPC-Staircase codes. The fact that LDPC-Staircase codes have been preferred to a major AL-FEC competitor for the ISDB-Tmm standard, is the recognition of their intrinsic qualities and of an appropriate balance between several technical and non technical criteria. See new results section for more details.
- We participate to The FIT project, 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. This 8-year project started in 2011 and will benefit from a 5.8 million euro grant from the French government. Its aims is to develop an experimental facility, a federated and competitive infrastructure with international visibility and a broad panel of customers. In the context of this project, are building a federated wireless testbed platform. See also http://fit-equipex.fr/.

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. In addition to our previous work, our focus is now on the monitoring of the Internet for the purpose of 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. This can be in the form of a pure disconnectivity, 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 traceroute, 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 will be to study to which extent one can troubleshoot the current Internet 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. 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. We are investigating a solution based on a two-layer signaling protocol a la ICMP in which edge routers are probed on end-to-end basis to collect local information on what is going on inside each network along the path. 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/Middelware: 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, Anasthesia Fedane.

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, Claudio Freire.

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 2011 we improved the robustness in the experiment control scheme, and we added support for new experimentation environments. We released and registered a second version of the NEPI software (IDDN.FR.001.06003.001.S.A.2010.000.10600). Details on the improvements made can be found in [48].
See also the web page http://nepihome.org.

- Version: 1.0
- 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.wikidot.com/
- Programming language: python

5.6. Reference implementation for SFA Federation of experimental testbeds

Participants: Thierry Parmentelat [correspondant], Baris Metin, 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. 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.

5.8. 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:

> to share IPR-free, open, AL-FEC codes, to share high performance, ready-to-use, open, free, C-language, software codecs and 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.

5.9. BitHoc

Participants: Chadi Barakat [correspondant], Thierry Turletti, Amir Krifa.

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 (http://www.alhem.net/Sockets/, GPL)
- Programming languages: C++, C#
- Documentation: doxygen

5.10. 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

5.11. Experimentation Software

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 in [41] 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: Rao Naveed Bin Rais, Chadi Barakat, Walid Dabbous, Damien Saucez, Jonathan Detchart, Mohamed Ali Kaafar, Amir Krifa, Ferdaouss Mattoussi, Vincent Roca, Thierry Turletti.

- **Disruption Tolerant Networking**

  We designed an efficient message delivery framework, called MeDeHa, which enables communication in an internet connecting heterogeneous networks that is prone to disruptions in connectivity[24]. MeDeHa is complementary to the IRTF's Bundle Architecture: besides its ability to store messages for unavailable destinations, MeDeHa can bridge the connectivity gap between infrastructure-based and multi-hop infrastructure-less networks. It benefits from network heterogeneity (e.g., nodes supporting more than one network and nodes having diverse resources) to improve message delivery. For example, in IEEE 802.11 networks, participating nodes may use both infrastructure- and ad-hoc modes to deliver data to otherwise unavailable destinations. It also employs opportunistic routing to support nodes with episodic connectivity. One of MeDeHa's key features is that any MeDeHa node can relay data to any destination and can act as a gateway to make two networks inter-operate or to connect to the backbone network. The network is able to store data destined to temporarily unavailable nodes till the time of their expiry. This time period depends upon current storage availability as well as quality-of-service needs (e.g., delivery delay bounds) imposed

by the application. We showcase MeDeHa's ability to operate in environments consisting of a diverse set of interconnected networks and evaluate its performance through extensive simulations using a variety of scenarios with realistic synthetic and real mobility traces. Our results show significant improvement in average delivery ratio and a significant decrease in average delivery delay in the face of episodic connectivity. We also demonstrate that MeDeHa supports different levels of quality-of-service through traffic differentiation and message prioritization.

Then, we have extended the MeDeHa framework to support multihop mobile ad-hoc networks (or MANETs). Integrating MANETs to infrastructure-based networks (wired or wireless) allows network coverage to be extended to regions where infrastructure deployment is sparse or nonexistent as well as a way to cope with intermittent connectivity. Indeed, to date there are no comprehensive solutions that integrate MANETs to infrastructure-based networks. We have proposed a message delivery framework that is able to bridge together infrastructure-based and infrastructure-less networks. Through extensive simulations, we have demonstrated the benefits of the extended MeDeHa architecture especially in terms of the extended coverage it provides as well as its ability to cope with arbitrarily long-lived connectivity disruptions. Another important contribution of this work is to deploy and evaluate our message delivery framework on a real network testbed as well as conduct experiments in "hybrid" scenarios running partly on simulation and partly on real nodes [32].

Finally, we have proposed a naming scheme for heterogeneous networks composed of infrastructure-based and infrastructure-less networks where nodes may be subject to intermittent connectivity. The proposed scheme, called Henna, aims at decoupling object identification from location and is designed to operate with status-quo Internet routing. We evaluated the proposed naming scheme using the ns-3 network simulator and demonstrated that nodes were able to receive messages in both infrastructure-based and infrastructure-less networks despite frequent disconnections and changing location identifiers (i.e., IP address), while visiting different networks [31].

Another important contribution of this work is to deploy and evaluate our message delivery framework on a real network testbed as well as conduct experiments in “hybrid” scenarios running partly on simulation and partly on real nodes. This was demonstrated at the ACM Sigcomm conference in Toronto on August 2011 [74].

These different works are the result of collaborations with Katia Obraczka and Marc Mendonca from University of California Santa Cruz (UCSC) in the context of the COMMUNITY Associated Team, see URL http://inrg.cse.ucsc.edu/community/.

Another activity in the same domain relates to efficient scheduling and drop policies in DTNs. We remind that Delay Tolerant Networks are 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. We are working on this extension within a new framework called MobiTrade, which 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. Using ns-3 simulations based on synthetic and real mobility traces, we show that MobiTrade achieves up to 2 times higher query success rates compared to other content dissemination schemes. Furthermore, we show that MobiTrade successfully isolates selfish devices. For further details on MobiTrade, we refer to [41] and to the web page of the project [1] where the code can be downloaded for both the ns-3 simulator and Android devices.

- **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 worked 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. This activity was started in October 2011 by Damien Saucez.

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

[1] http://planete.inria.fr/MobiTrade/

With the advent of broadcast/multicast systems (e.g., DVB-H/SH), 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 recent activities, in the context of the PhD of F. Mattoussi, included 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, while keeping backward compatibility (LDPC-Staircase "codewords" can be decoded with a GPLDPC-Staircase codec).

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. This is the first adoption of these codes in an international standard.

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 a recent Internet-Draft [66] defines 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 of 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, will be commercialized in 2012 through an industrial partner. This codec proves that LDPC-Staircase codes can offer erasure recovery performances close to ideal codes in many circumstances while keeping decoding speeds over 1Gbps.

The fact that LDPC-Staircase codes have been preferred to a major AL-FEC competitor for the ISDB-Tmm standard, is the recognition of their intrinsic qualities and of an appropriate balance between several technical and non technical criteria.

- **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 [65] 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 [66], [65].

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 [67]. 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 RFC [68].

  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: [59] [60] [61].

  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, in [29]. 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 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. 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[56], [57], [58].

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

  We believe that sooner or later, broadcasting systems will require security services. This is all the more true as heterogeneous broadcasting technologies will be used, for instance hybrid satellite-based and terrestrial networks, some of them being by nature open, as wireless networks (e.g., wimax, wifi). Therefore, one of the key security services is the authentication of the packet origin, and the packet integrity check. A key point is the ability for the terminal to perform these checks easily (the terminal often has limited processing and energy capabilities), while being tolerant to packet losses.

The TESLA (Timed Efficient Stream Loss-tolerant Authentication) scheme fulfills these requirements. We are therefore standardizing the use of TESLA in the context of the ALC and NORM reliable multicast transport protocols, within the IETF MSEC working group. This document has been published as RFC 5776.

In parallel, 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 in [62], [63], [64]. This activity is also carried out within the IETF RMT working group.

- **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 has 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.

6.2. Network Security and Privacy

Participants: Sana Ben Hamida, Claude Castelluccia, Walid Dabbous, Mohamed Ali Kaafar, Arnaud Legout, Stevens Le Blond, Daniele Perito.

- **Online users tracking and profiling techniques**

  Usernames are ubiquitously used for identification and authentication purposes on web services and the Internet at large, ranging from the local-part of email addresses to identifiers in social networks. Usernames are generally alphanumerical strings chosen by the users and, by design, are unique within the scope of a single organization or web service. In this work, we investigate the feasibility of using usernames to trace or link multiple profiles across services that belong to the same individual. The intuition is that the probability that two usernames refer to the same physical person strongly depends on the entropy of the username string itself. Our experiments, based on usernames gathered from real web services, show that a significant portion of the users' profiles can be linked using their usernames. In collecting the data needed for our study, we also show that users tend to choose a small number of related usernames and use them across many services. This work is the the first to consider usernames as a source of information when profiling users on the Internet. It has been published in PETS 2011 [47], one of the most prestigious conference in the area of Computer Privacy, and has been awarded the Andreas Pfitzmann award for the best contribution.

- **Online Privacy measurements and threats identification in online social networks**

In this work, 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 friends relationship 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. To the best of our knowledge, this is the first time that user interests are used for profiling, and more generally, semantics-driven inference of private data is addressed. This work has been published in the prestigious Network & Distributed System Security Symposium (NDSS) 2012 [37].

- **Privacy Enhancing Technologies**

  The increasing amount of personal and sensitive information disseminated over the Internet prompts commensurately growing privacy concerns. Digital data often lingers indefinitely and users lose its control. This motivates the desire to restrict content availability to an expiration time set by the data owner. This work presents and formalizes the notion of Ephemeral Publishing (EphPub), to prevent the access to expired content. We propose an efficient and robust protocol that builds on the Domain Name System (DNS) and its caching mechanism. With EphPub, sensitive content is published encrypted and the key material is distributed, in a steganographic manner, to randomly selected and independent resolvers. The availability of content is then limited by the evanescence of DNS cache entries. The EphPub protocol is transparent to existing applications, and does not rely on trusted hardware, centralized servers, or user proactive actions. We analyze its robustness and show that it incurs a negligible overhead on the DNS infrastructure. We also perform a large-scale study of the caching behavior of 900K open DNS resolvers. Finally, we propose an Android application, Firefox and Thunderbird extensions that provide ephemeral publishing capabilities, as well as a command-line tool to create ephemeral files. This work has been published in ICNP 2011 [36].

- **Differentially private smart metering**

  Several countries throughout the world are planning to deploy smart meters in households in the very near future. The main motivation, for governments and electricity suppliers, is to be able to match consumption with generation. Traditional electrical meters only measure total consumption on a given period of time (i.e., one month or one year). As such, they do not provide accurate information of when the energy was consumed. Smart meters, instead, monitor and report consumption in intervals of few minutes. They allow the utility provider to monitor, almost in realtime, consumption and possibly adjust generation and prices according to the demand. Although smart metering might help improving energy management, it creates many new privacy problems. Smart meters provide very accurate consumption data to electricity providers. As the interval of data collected by smart meters decreases, the ability to disaggregate low-resolution data increases.

  We developed a new privacy-preserving smart metering system. Our scheme is private under the differential privacy model and therefore provides strong and provable guarantees. With our scheme, an (electricity) supplier can periodically collect data from smart meters and derive aggregated statistics while learning only limited information about the activities of individual households. For example, a supplier cannot tell from a user's trace when he watched TV or turned on heating. Our scheme is simple, efficient and practical. Processing cost is very limited: smart meters only have to add noise to their data and encrypt the results with an efficient stream cipher.

This work was presented at IH'11 (the Information Hiding Conference, 2011) [34].

- **Protecting against Physical Resource Monitoring**

  This work considers the problem of resource monitoring. We consider the scenario where an adversary is physically monitoring on the resource access, such as the electricity line or gas pipeline, of a user in order to learn private information about his victim. Recent works, in the context of smart metering, have shown that a motivated adversary can basically profile a user or a family solely from his electricity traces. However, these works only consider the case of a semi-honest-but-non-intrusive adversary that is only trying to learn information from the consumption reports sent by the user. This work, instead, considers the much more challenging case of a intrusive semi-honest adversary, i.e. a semi- honest adversary that is in addition physically monitoring the resource by modifying the distribution network. We aim at answering to the following question: is it possible to design a resource distribution scheme that prevents resource monitoring and provides strong protection? We propose and analyze several possible solutions. The proposed solutions provide different privacy bounds and performance results. This work was presented at WPES'11 (ACM Workshop on Privacy in the Electronic Society) [35].

- **The Failure of Noise-Based Non-Continuous Audio Captchas**

  CAPTCHAs, which are automated tests intended to distinguish humans from programs, are used on many web sites to prevent bot-based account creation and spam. To avoid imposing undue user friction, CAPTCHAs must be easy for humans and difficult for machines. However, the scientific basis for successful CAPTCHA design is still emerging. This project examines the widely used class of audio CAPTCHAs based on distorting non-continuous speech with certain classes of noise and demonstrates that virtually all current schemes, including ones from Microsoft, Yahoo, and eBay, are easily broken. More generally, we describe a set of fundamental techniques, packaged together in our Decaptcha system, that effectively defeat a wide class of audio CAPTCHAs based on non-continuous speech. Decaptcha's performance on actual observed and synthetic CAPTCHAs indicates that such speech CAPTCHAs are inherently weak and, because of the importance of audio for various classes of users, alternative audio CAPTCHAs must be developed.

  This work was presented at IEEE Security and Privacy 2011 [33].

- **BlueBear: Privacy in P2P systems**

  We have started a new project called bluebear on privacy threats in the Internet. Indeed, the Internet has never been designed with privacy in mind. For instance, the Internet is based on the IP protocol that exposes the IP address of a user to any other users it is communicating with. However, we believe that current users of the Internet do not realize how much they compromise their privacy by using the Internet. Indeed, the common wisdom is that there are so many users in the Internet that it is not feasible for an attacker, apart may be for national agencies, to globally compromise the privacy of a large fraction of users. Therefore, finding a specific user is like looking for a needle in a haystack. The goal of the bluebear project is to raise attention on privacy issues when using the Internet. In particular, we want to show that without any dedicated infrastructure, it is possible to globally compromise the privacy of Internet users. BitTorrent is arguably the most efficient peer-to-peer protocol for content replication. However, BitTorrent has not been designed with privacy in mind and its popularity could threaten the privacy of millions of users.

In a first study we showed that it is possible to continuously monitor from a single machine most BitTorrent users and to identify the content providers (also called initial seeds). We performed a very large monitoring operation continuously "spying" on most BitTorrent users of the Internet from a single machine and for a long period of time. During a period of 103 days, we collected 148 million IP addresses downloading 2 billion copies of contents. We then identified the IP address of the content providers for 70% of the BitTorrent contents we spied on. We showed that a few content providers inject most contents into BitTorrent and that those content providers are located in foreign data centres. We also showed that an adversary could compromise the privacy of any peer in BitTorrent and identify the big downloaders that we define as the peers who subscribe to a large number of contents. This is a major privacy threat as it is possible for anybody in the Internet to reconstruct all the download and upload history of most BitTorrent users. This work was published in LEET 2010.

To circumvent this kind of monitoring, BitTorrent users are increasingly using anonymizing networks such as TOR to hide their IP address from the tracker and, possibly, from other peers. We explored in a second study whose goal was to Exploit P2P Applications to Trace and Profile Tor Users, to which extent a P2P protocol such as BitTorrent, when not designed to protect users information, leak information that may compromise the identity of users. We quantified such an issue with BitTorrent on top of anonymizing networks. We also designed an attack that reveals the identity of Tor users (We showed that it is possible to retrieve the IP address for more than 70% of BitTorrent users on top of TOR). Moreover, once the IP address of a peer is retrieved, it is possible to link to the IP address other applications used by this peer on top of TOR [45].

The fact that it is hard for a person to map an IP address to an identity mitigates the impact of the privacy attacks we described. However, we show that we can exploit a peer-to-peer VoIP system to associate a social identity (name, email address, etc.) to an IP address [46]. This means that anybody can now find this mapping that was only known by ISPs or big companies (like Google and Facebook), but never communicated unless in case of a legal action. The privacy threat is thus very high because this mapping enables blackmail, social attacks, targeted phishing attacks, etc.

As a proof of concept, we show that it is possible to track VoIP users mobility and BitTorrent downloads [46] using Skype, one of the most popular VoIP system with more that 500 millions registered users.

All these works received a very large media coverage (see http://www-sop.inria.fr/members/Arnaud.Legout/Projects/bluebear.html).

6.3. Network measurement, modeling and understanding

Participants: Chadi Barakat, Roberto Cascella, Mohamed Ali Kaafar, Imed Lassoued, Arnaud Legout, Ashwin Rao, Mohamad Jaber, Amir Krifa, Mauricio Jost.

The main objective of our work in this domain is a better monitoring of the Internet and a better control of its resources. 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 ECODE FP7 project, we work on a network-wide monitoring architecture that, given a measurement task to perform, tune the monitors inside the network optimally so as to maximize the accuracy of the measurement results while limiting the overhead resulting from collected traffic. 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.

- **Internet traffic classification by means of packet level statistics**

  One of the most important challenges for network administrators is the identification of applications behind the Internet traffic. This identification serves for many purposes as in network security, traffic

engineering and monitoring. The classical methods based on standard port numbers or deep packet inspection are unfortunately becoming less and less efficient because of encryption and the utilization of non standard ports. In this activity, we come up with an online iterative probabilistic method that identifies applications quickly and accurately by only using the size of packets. Our method associates a configurable confidence level to the port number carried in the transport header and is able to consider a variable number of packets at the beginning of a flow. By verification on real traces we observe that even in the case of no confidence in the port number, a very high accuracy can be obtained for well known applications after few packets were examined. In another work [39], we make a complete study about the inter-packet time to prove that it is also a valuable information for the classification of Internet traffic. We discuss how to isolate the noise due to the network conditions and extract the time generated by the application. We present a model to preprocess the inter-packet time and use the result as input to the learning process. We discuss an iterative approach for the on line identification of the applications and we evaluate our method on two different real traces. The results show that the inter-packet time is an important parameter to classify Internet traffic.

We pursued this activity further by accounting for the communication profiles of hosts for the purpose of a better traffic classification [39], [38], [40]. We use the packet size and the inter-packet time as the main features for the classification and we benefit from the traffic profile of the host (i.e. which application and how much) to refine the classification and decide in favor of this or that application. The host profile is then updated online based on the result of the classification of previous flows originated by or addressed to the same host. We evaluate our method on real traces using several applications. The results show that leveraging the traffic pattern of the host ameliorates the performance of statistical methods. They also prove the capacity of our solution to derive profiles for the traffic of Internet hosts and to identify the services they provide.

For a more thorough study of the traffic classification problem by means of packet statistics and host profiles, we refer to the PhD dissertation of Mohamad Jaber who was the main contributor to this activity inside the EPI Planete.

- **Adaptive network-wide traffic monitoring**

  The remarkable growth of the Internet infrastructure and the increasing heterogeneity of applications and users' behavior make more complex the manageability and monitoring of ISP networks and raises the cost of any new deployment. The main consequence of this trend is an inherent disagreement between existing monitoring solutions and the increasing needs of management applications. In this context, we work on the design of an adaptive centralized architecture that provides visibility over the entire network through a network-wide cognitive monitoring system. Given a measurement task, the proposed system drives its own configuration, typically the packet and flow sampling rates in routers, in order to address the tradeoff between monitoring constraints (processing and memory cost, collected data) and measurement task requirements (accuracy, flexibility, scalability). We motivate our architecture with an accounting application: estimating the number of packets per flow, where the flow can be defined in different ways to satisfy different objectives (e.g., Domain-to-Domain traffic, all traffic originated from a domain, destined to a domain). The architecture and the algorithms behind it are explained in paper published in 2010 for the case of a proactive control and in [43] for the case of a reactive control. In [44] the architecture and its algorithms are specified to a flow counting application. In all these works, the performances of our architecture are being validated in typical scenarios over an experimental platform we developed for the purpose of the study. Our platform is called MonLab (Monitoring Lab) and is described with more details in the Section on produced softwares. For now, MonLab presents a new approach for the emulation of Internet traffic and for its monitoring across the different routers. It puts at the disposal of users a real traffic emulation service coupled to a set of libraries and tools capable of Cisco NetFlow data export and collection, the overall destined to run advanced applications for network-wide traffic monitoring and optimization.

The activities in this direction are funded by the ECODE FP7 STREP project (Sep. 2008 - Dec. 2011). The dissertation of Imed Lassoued [21] provides an introduction to the field in addition to details on our contributions and the MonLab emulation platform.

- **Spectral analysis of packet sampled traffic**

  In network measurement systems, packet sampling techniques are usually adopted to reduce the overall amount of data to collect and process. Being based on a subset of packets, they hence introduce estimation errors that have to be properly counteracted by a fine tuning of the sampling strategy and sophisticated inversion methods. This problem has been deeply investigated in the literature with particular attention to the statistical properties of packet sampling and the recovery of the original network measurements. Herein, we propose a novel approach to predict the energy of the sampling error on the real time traffic volume estimation, based on a spectral analysis in the frequency domain. We start by demonstrating that errors due to packet sampling can be modeled as an aliasing effect in the frequency domain. Then, we exploit this theoretical finding to derive closed-form expressions for the Signal-to-Noise Ratio (SNR), able to predict the distortion of traffic volume estimates over time. The accuracy of the proposed SNR metric is validated by means of real packet traces. The analysis and the expressions of the SNR that stemmed from are described in [26]. In [52], we adopt such a model to design a real-time algorithm, that sets the IPFIX counter export timers in order to grant, to each flow, a target estimation accuracy. The work within this direction has been partially supported by the FP7 ECODE project.

- **Monitoring the quality of the Internet access by end-to-end probes**

  The detection of anomalous links and traffic is important to manage the state of the network. Existing techniques focus on detecting the anomalies but little attention has been devoted to quantify to which extent network anomaly affects the end user access link experience. We refer to this aspect as the *local seriousness* of the anomaly. In order to quantify the local seriousness of an anomaly, we consider the percentage of affected destinations, that we call the *impact factor*. In order to measure it, a host should monitor all possible routes to detect any variation in performance, but this is not practical in reality. In this activity, funded by the ANR CMON project, we work on finding estimates for the impact factor and the local seriousness of network anomalies through a limited set of measurements to random nodes we call landmarks.

  We initially study the user access network to understand the typical features of its connectivity tree. Then, we define an unbiased estimator for the local seriousness of the anomaly and a framework to achieve three main results: *(i)* the computation of the minimum number of paths to monitor, so that the estimator can achieve a given significance level, *(ii)* the localization of the anomaly in terms of hop distance from the local user, and *(iii)* the optimal selection of landmarks. We are using real data to evaluate in practice the local seriousness of the anomaly and to determine the sufficient number of landmarks to select randomly without knowing anything on the Internet topology. The localization mechanism leverages the study on the connectivity tree and the relationship between the impact factor and the minimum hop distance of an anomaly. Our first results show that the impact factor is indeed a meaningful metric to evaluate the quality of Internet access. The current work focuses on extending this solution towards a collaborative setting where different end users collaborate together by exchanging the results of their observations. The objective will be a better estimation of the impact factor by each of them and a finer localization of the origin of any network problem.

On the experimental side, we have implemented the solution in a tool called ACQUA, which stands for Application for Collaborative Estimation of QUality of Internet Access [2]. We design an anomaly detection mechanism based on the histogram of delay measurements and the likelihood of observations. Then, we give to ACQUA a pipeline based software architecture, and we go deeply into experimentation inside and outside Planetlab. We show what the properties and usage of the algorithm are, focusing also on how this tool can help us to get information about the network anomalies detected. Later we extend the idea of Impact Factor Estimation (IFE) by using what we call Inverse IFE from Planetlab, where the computer of the user whose connectivity is tested has a completely passive role in the measurements procedure. We study its strong and weak points, and we show conditions under which Inverse IFE from Planetlab gives similar results to traditional IFE.

- **Applied Internet Measurements**

  The performance of several Internet applications often relies on the measurability of path similarity between different participants. In particular, the performance of content distribution networks mainly relies on the awareness of content sources topology information. It is commonly admitted nowadays that, in order to ensure either path redundancy or efficient content replication, topological similarities between sources is evaluated by exchanging raw traceroute data, and by a hop by hop comparison of the IP topology observed from the sources to the several hundred or thousands of destinations. In this project, based on real data we collected, we advocate that path similarity comparisons between different Internet entities can be much simplified using lossy coding techniques, such as Bloom filters, to exchange compressed topology information. The technique we introduce to evaluate path similarity enforces both scalability and data confidentiality while maintaining a high level of accuracy. In addition, we demonstrate that our technique is scalable as it requires a small amount of active probing and is not targets dependent. This work has been published in [25].

- **Reliability of Geolocation Databases**

  In this project, we question the reliability of geolocation databases, the most widely used technique for IP geolocation. It consists in building a database to keep the mapping between IP blocks and a geographic location. Several databases are available and are frequently used by many services and web sites in the Internet. Contrary to widespread belief, geolocation databases are far from being as reliable as they claim. We conduct a comparison of several current geolocation databases -both commercial and free- to have an insight of the limitations in their usability. First, the vast majority of entries in the databases refer only to a few popular countries (e.g., U.S.). This creates an imbalance in the representation of countries across the IP blocks of the databases. Second, these entries do not reflect the original allocation of IP blocks, nor BGP announcements. In addition, we quantify the accuracy of geolocation databases on a large European ISP based on ground truth information. This is the first study using a ground truth showing that the overly fine granularity of database entries makes their accuracy worse, not better. Geolocation databases can claim country-level accuracy, but certainly not city-level. This study has been published in CCR [28].

- **Impact of Live Streaming Traffic**

[2] http://planete.inria.fr/acqua/

Video streaming is the most popular traffic in the Internet and a strong case for content centric networks. Therefore, it is fundamental to understand the network traffic characteristics of video streaming. In this work [49], we extensively studied the network traffic characteristics of YouTube and Netflix (the most popular video streaming traffic in the USA). We have shown that the traffic characteristics vastly depends on the type of browser, mobile application, and container (Flash, Silverlight, HTLM5) used.

6.4. Experimental Environment for Future Internet Architecture

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

- **SFA Federation of experimental testbeds**

  The OneLab2 project has come to its end in spring 2010. We are now involved in the NOVI (E.U. STREP) project, the F-Lab (French A.N.R.) project, and have the lead of the "Federation" WorkPackage of OpenLab (E.U. IP) project. Within these frameworks, we are codevelopping with Princeton University a reference implementation for 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 2011 we have focused on the maturation of the SFA codebase, with several objectives in mind. Firstly we have contributed to a major overhaul of the specification as defined essentially within the GENI (N.S.F.) Project, with participations from all over the world. These changes, that affected both the core API and the schema used to expose and manage resource specifications, aimed at reaching a mature level of interoperabity between the PlanetLab world and the EmuLab a.k.a. ProtoGeni world that has its own implementation, and are now available in SFA-2.0 issued late 2011.

  Secondly, the SFA codebase has been redesigned to provide a more generic shelter that other testbeds can easily leverage in order to come up with their own SFA-compliant wrapper. This is perceived as a powerful means to foster further adoption of the architecture, and the Planète team has been intrumental in bringing two entirely different testbeds to the federation, namely Senslab - developped in other INRIA Project-teams - and FEDERICA, the outcome of another E.U.-funded Project. Along the same lines we are working, although more remotely, with NICTA in Australia that publishes the O.M.F. testbed for running wireless testbeds, and who are interested in adopting this federation paradigm.

  Finally, as part of the pure PlanetLab development, we have added a feature for running nodes in a 'reservable' mode, which breaks the usual best-effort PlanetLab model, but turned out very helpful both for making experiments possible, that needed a more reproducible behaviour of experiments, and also in a federation perspective, for closing the usage gap with, notably wireless testbeds, that typically have a reservable-only provisioning mechanisms.

- **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.

- **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.

- **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. This web site is now finalized. However, activities related to developing the consortium have slowed down during 2011 due to the leave of Mathieu Lacage. We plan to put more resources on this aspect in 2012.

- **Using Independent Simulators, Emulators, and Testbeds for Easy Experimentation**

  Evaluating new network protocols, applications, and architectures uses many kinds of experimentation environments: simulators, emulators, testbeds, and sometimes, combinations of these. As the functionality and complexity of these tools increases, mastering and efficiently using each of them is becoming increasingly difficult.

We designed the preliminary prototype of the Network Experiment Programming Interface (NEPI) whose goal is to make easier the use of different experimentation environments, and switch among them easily. NEPI intends to make it possible to write a single script to control every aspect of a potentially mixed experiment, including a hierarchical network topology description, application-level setup, deployment, monitoring, trace setup, and trace collection. We showed how a single object model which encompasses every aspect of a typical experimentation workflow can be used to completely describe experiments to be run within very different experimentation environments. 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. Last year, 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. This year we have 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. The NEPI approach has been validated by implementing support for three complementary environments: a physical testbed, a network emulator, and a network simulator. Furthermore, we showed with a concrete experiment use case, available online for reproduction, how easy it is with NEPI to integrate these environments for hybrid-experimentation [48].

- **Guidelines for the accurate design of empirical studies in wireless networks**

  Traditionally, wireless protocol proposals have been often tested and validated using only analytical and simulation models [73]. However, as the wireless environment is very complex to model accurately, and since the cost of wireless cards has decreased in an exponential way, today more and more research papers include evaluation of new proposals using experimentation on real devices. Indeed, experimentation is a mandatory step before possible deployment of new network protocols with real users. However, wireless experimentation is much more complex to set up and run than simulation, and it is important to avoid many pitfalls that can occur during experimentation. The objectives of this work are twofold. First, we described typical problems currently encountered in wireless-based experimentation, and we presentd simple guidelines to avoid them [50]. Second, we proposed an experimental methodology where the detection of anomalies, calibration of the measurement setup, and clear definition of the scenario (among others) make easier the repeatability of results [55]. This work has been done in collaboration with Cristian Tala, Luciano Ahumada and Diego Dujovne from the Universidad Diego Portales of Chili, in the context of the WELCOME STIC AMSud 2011.

- **Multicast Video Streaming over WiFi Networks: Impact of Multipath Fading and Interference**

  We conducted an experimental study in order to analyse the impact of interference, multipath fading and path loss on multicast video streaming (i.e., goodput, packet loss and ultimately on the video quality) using off-the-shelf fixed WiFi equipment in a wireless (802.11 b/g) local area network (WLAN) environment. We used the ricean K-factor as a measure of multipath fading, spectrum analyzer to estimate channel interference and received signal strength indicator (RSSI) as indication of signal power and attenuation. In order to realistically measure forementioned metrics, we conducted extensive wireless experiments against six test cases representing common real-world situations using off-the-shelf wireless equipment.

We showed that interference has more impact on performance than multipath fading. Multipath fading can result in considerable performance degradation in environments where moving objects cause perturbance. On the contrary, channel interference is more frequent and more prominent cause of performance degradation in wireless networks because ISM 2.4 GHz band is increasingly being utilized in homes and work places. Being able to quantify the impact of multipath fading and interference is crucial in planning, troubleshooting, managing as well as benchmarking and optimizing wireless networks. This study has been pusblished in MediaWin 2011 [51].

- **Making easier Experimentation**

  Wireless experimentations are challenging to evaluate due to the high variability of the channel characteristics and its sensitivity to interferences.

  Merging traces represents a complex problem especially in wireless experimentations, due to packet redundancy in multiple probes. Merging traces solutions need to be efficient in order to process the large amount of generated traces. These solutions should provide an output data structure that allows easy and fast analysis and must be scalable in order to be used in large and various experimental settings. We have designed an algorithm that performs trace synchronization and merging in a scalable way. The algorithm output is stored in a configured MYSQL database allowing for smart packet trace storage. This solution reduces processing time by 400% and storage space by 200% with regard to raw trace file solutions. It has been implemented in an open source software called CrunchXML, available under the GNU General Public License v2 at http://twiki-sop.inria.fr/twiki/bin/view/Projets/Planete/CrunchXML.

- **An Integration Framework for Network Experimentation**

  Many different experimentation environments address complementary aspects of network protocol evaluation, but because of their disparities and complexities it is often hard to use them to reproduce the same experiment scenario.

  Simulation is often used for the evaluation of new network protocols and architectures. In order to perform more realistic simulations, modern simulators such as ns-3 integrate more detailed models and even support direct execution of real protocol code. However, such complex models require more computational and memory requirements. We have studied the feasibility of a hybrid approach based on distributing a complex simulation scenario on several nodes in a grid network. We showed that by exploiting the real time operation of the ns-3 simulator, it is possible to map such complex scenarios on grid nodes. We also proposed a basic mapping algorithm to distribute a simulation scenario in several nodes [42].

7. Contracts and Grants with Industry

7.1. Contracts with Industry

Industrial contract with Alcatel Lucent - Bell Labs (2008-2011):

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.

7.2. Grants with Industry

CEA LETI, Grenoble (2008-2011):
CEA LETI is providing a phd grant to support the activity on wireless sensor network security. This grant supports Sana Ben Hamida.

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. ECODE

Title: Experimental COgnitive Distributed Engine

Type: COOPERATION (ICT)

Defi: New paradigms and experimental facilities

Instrument: Specific Targeted Research Project (STREP)

Duration: September 2008 - August 2011

Coordinator: Alcatel Lucent (Belgium)

Others partners: UCL (Belgium), ULg (Belgium), IBBT (Belgium), ULANC (UK), CNRS (France).

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

Abstract: The goal of the ECODE project is to develop, implement, and validate experimentally a cognitive routing system that can meet the challenges experienced by the Internet in terms of manageability and security, availability and accountability, as well as routing system scalability and quality. By combining both networking and machine learning research fields, the resulting cognitive routing system fundamentally revisits the capabilities of the Internet networking layer so as to address these challenges altogether. For this purpose, the project investigates and elaborates novel semi-supervised, on line, and distributed machine learning techniques kernel of the cognitive routing system. During the building phase, the cognitive routing system is both designed and prototyped. In the second phase, three sets of use cases are experimented to evaluate the benefits of the developed machine learning techniques. The experimentation and the validation of these techniques are carried out on physical (iLAB) and virtual (e.g.,OneLab) experimental facilities.

8.3.1.2. 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.

8.3.1.3. 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. WSN4CIP

Title: Wireless Sensor Networks for critical infrastructures Protection

Type: COOPERATION (ICT)

Defi: FP7 Security area, Objective 1.7 Critical Infrastructure Protection

Instrument: Specific Targeted Research Project (STREP)

Duration: 2009 - 2011

Coordinator: Eurescom (Germany)

Others partners: 11 European partners (including IHP, NEC, BUTE, etc.)

See also: http://www.wsan4cip.eu/home.html

Abstract: The goal of WSAN4CIP is to advance the technology of Wireless Sensor and Actuator Networks (WSANs) beyond the current state of the art, in order to improve the protection of Critical Infrastructures (CIs) By advancing WSAN technology, the project contributes to networked information and process control systems which are more secure and resilient. The distributed nature of WSANs enables them to survive malicious attacks as well as accidents and operational failures. It makes them dependable in critical situations, when information is needed to prevent further damage to CIs.

8.3.2. EIT KIC funded activities

Our project team was involved in 2011 in two activities funded by the EIT ICT Labs KIC: FITTING on Future InterneT (of ThINGs) facility and Information centric and device clouds (11901). In 2012, we will be involved in three additional activities on Software-Defined Networking (SDN) (11634), Information-centric networking (ICN) experimentation (12191) and Seamless P2P video streaming for the web (12199). The FITTING activity is mentioned as a "success story" by the EIT ICT Labs KIC [3]. 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.

8.3.2.1. FITTING

Title: Future InterneT (of ThINGs) facility

Activity Number: 10340

Duration: 2011-2012

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

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

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.

8.4. International Initiatives

8.4.1. INRIA Associate Teams

COMMUNITY Associated team (2009-2011): Planète is an associated team with the UC Santa Cruz's Jack Baskin School of Engineering. The collaborative project is about communication in heterogeneous networks prone to episodic connectivity, see URL http://inrg.cse.ucsc.edu/community/. Our initial scientific objective throughout the project was to design efficient message delivery mechanisms for challenged and heterogeneous networks, and targeted:

- The design of a unifying solution to enable message delivery over heterogeneous networks with varying degrees of connectivity.
- The design of error- and congestion control techniques in episodically connected networks.
- The exploration of different mechanisms for quality-of-service (QoS) support in such environments.

We have re-oriented some of the initial proposed research. In particular, rather than investigating error and congestion control techniques for DTNs, we focused on the development of efficient routing strategies that take into account the *utility* of nodes to relay messages. Furthermore, we developed a naming scheme that supports message delivery over heterogeneous networks prone to connectivity disruptions, see further details in Section 1.

8.4.2. Visits of International Scientists

Luigi Alfredo Grieco, Visiting Professor (one week in December 2011)

Subject: On Evaluating Fairness in Content Centric Networks

Institution: University of Bari (Italy)

Katia Braczka, Visiting Professor (one week in January 2011 and one week in November 2011)

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 2011 until Dec 2011)

Subject: Efficient Communication Mechanisms for Episodically Connected and Heterogeneous Networks

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

8.4.3. Visits to International teams

Thierry Turletti, Visiting researcher to University of California at Santa Cruz (one week in June 2011)

Subject: Efficient Communication Mechanisms for Episodically Connected and Heterogeneous Networks

8.4.4. Participation In International Programs

- WELCOME (STIC AmSud): This project (2010-2011) aims to design realistic models of the physical layer in order to be used in both simulations and experimentation of wireless protocols. In addition to the Planète Project-Team, the partners are Universidad de Valparaiso, Chile, Universidad de Córdoba, Argentina and Universidad Diego Portales, Chile.
- 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.

9. Dissemination

9.1. Animation of the scientific community

Walid Dabbous served in the programme committees of WNS3'2011, NOMEN'2012, ICC'12 NGN. He is co-editor or a special issue of the PPNA journal on Experimental Evaluation of Peer-to-Peer Applications. He is member of the scientific council of the INRIA Bell-Labs laboratory on Self Organizing Networks. He is an affiliate professor at Ecole Polytechnique, Palaiseau.

Claude Castelluccia served in the program committees of the following international conferences: Wisec2011 and SESOC2011. He is the co-founder of the ACM WiSec (Wireless Security) conference.

Thierry Turletti Senior ACM and IEEE member, served in 2011 in the program committees of the following international conferences: 19th International Packet Video Workshop and 4th 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 is General Co-Chair of the upcoming ACM CoNEXT 2012 conference on emerging Networking EXperiments and Technologies to be held in Nice on Dec 10-13, 2012. He served on the Technical Program Committee for IEEE Infocom 2011 and ACM CoNEXT 2011. He was invited to give talks at the CFIP Conference in Sainte Maxime - 2011. 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 in the RMT, FECFRAME and MSEC working groups at the IETF (he was in particular co-chair of the MSEC, Multicast Security working group in 2010-2011).

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 2011, he served in the program committees of the following international conferences: Security, Inforensics and Cyber Criminality 2011, CCSEIT-2011, ACC 2011, IWTMP2PS 2011. He is member of the steering commitee of Colloque Jacques Cartier : Security, Inforensics and Cyber Criminality. He is member of the editorial board of IEEE Transactions on Parallel and Distributed Systems TPDS, Computer Communications, IEEE letters of communications, Computer Networks, the International Journal of peer-to-peer networks (IJP2P).

9.2. Teaching

9.2.1. Teaching Activities

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 (12h), 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 RTM: course on Wireless networking by Chadi Barakat, 7h, IUP Avignon, 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.

9.2.2. Phd students

PhD : Daniele Perito defended his PhD titled "Trustworthy Code Execution on Embedded Devices" on October 13th, at Grenoble University. His thesis was supervised by Claude Castelluccia.

PhD: Stevens Le Blond defended his PhD titled "Is Privacy Dead (in P2P Networks)?" on April 28th. His thesis was co-supervised by Arnaud Legout and Walid Dabbous.

PhD: Rao Naveed Bin Rais defended his PhD titled "Adaptive Communication Mechanisms for Networks with Episodic Connectivity" on February 1st, at University of Nice-Sophia Antipolis. His thesis was supervised by Thierry Turletti.

PhD : Mohamad Jaber defended his PhD titled "Internet traffic profiling and identification" on October 6th at University of Nice-Sophia Antipolis. His thesis was supervised by Chadi Barakat.

PhD: Imed Lassoued defended his PhD titled "Adaptive Monitoring and Management of Internet Traffic" on December 13 at University of Nice-Sophia Antipolis. His thesis was supervised by Chadi Barakat.

PhD in progress : Sana Ben Hamida works on "Embedded System Security" since 2009. Her thesis is 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 : 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: Anshuman Kalla works on “Efficient transmission mechanisms for Information Centric Network Architectures” since december 2011. His thesis is co-supervised by Thierry Turletti and Walid Dabbous.

PhD in progress: Shafqat Ur-Rehman works on “Benchmarking in Wireless Networks” since 2008. His thesis is co-supervised by Thierry Turletti and Walid Dabbous.

PhD in progress: Amir Krifa works on “Towards better content dissemination applications for Disruption Tolerant Networks” since 2009. His thesis is supervised by Chadi Barakat.

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 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 2010. Her work is co-supervised by Vincent Roca and Bessem Sayadi.

9.2.3. Interns

Ana Nika (from Mar 2011 until Jul 2011)

Subject: Henna: A new naming mechanism for very heterogeneous networks prone to connection disruptions

Institution: National University of Athens (Greece)

Claudio Freire (from March 2011 until Sep 2011)

Subject: Extending NEPI, Adding support for PlanetLab experimentation platform

Institution: Universidad de Buenos Aires (Argentina)

Sandun Wijayarathne (from April 2011 to August 2011)

Subject: Support of mobility in content centric networks

Institution: Ubinet Master, University of Nice-Sophia Antipolis (France)

Mauricio Jost (from April 2011 to August 2011)

Subject: Monitoring the quality of internet access by active probing

Institution: Ubinet Master, University of Nice-Sophia Antipolis (France)

Blerina Lika (from June 2011 to July 2011)

Subject: Rate and error control in content centric network

Institution: National University of Athens (Greece)

Anestasia Fedane (from Feb 2011 to July 2011)

Subject: Privacy in Location-Based Services

Institution: University of Grenoble (France)

Min-Dung Tran (from Feb 2011 to July 2011)

Subject: Information Leakage in Ad systems

Institution: University of Grenoble (France)

William Lecat (from April 2011 to June 2011)

Subject: Differentially private spatial aggregation

Institution: Ecole Polytechnique (France)

Hervé Falciani (from March 2011 to August 2011)

Subject: Personal Data on Content Centric Networking

Institution: Ubinet Master, University of Nice-Sophia Antipolis (France)

Manu Sekar (from Feb 2011 to July 2011)

Subject: Energy versus Security tradeoff in Wireless Sensor Networks

Institution: INPG (France)

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)", April 2010, http://arxiv.org/abs/1004.5217.

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

[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] 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.

[12] 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.

[13] 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.

[14] 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).

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

[16] 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^{o} 8.

[17] 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^{o} 8.

[18] 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

[19] R. N. BIN RAIS. *Communication Mechanisms for Message Delivery in Heterogeneous Networks Prone to Episodic Connectivity*, Université de Nice Sophia-Antipolis, February 2011, http://hal.inria.fr/tel-00590626/en.

[20] M. JABER. *Internet Traffic Profiling and Identification*, Université de Nice Sophia Antipolis, October 2011.

[21] I. LASSOUED. *Adaptive Monitoring and Management of Internet Traffic*, Université de Nice Sophia Antipolis, December 2011.

[22] S. LE BLOND. *Is Privacy Dead (in P2P Networks)?*, Université de Nice Sophia Antipolis, April 2011.

[23] D. PERITO. *Exécution sécurisée de code sur systèmes embarqués*, Université de Grenoble, October 2011, http://hal.inria.fr/tel-00639053/en.

Articles in International Peer-Reviewed Journal

[24] R. N. BIN RAIS, T. TURLETTI, K. OBRACZKA. *Message Delivery in Heterogeneous Networks prone to Episodic Connectivity*, in "ACM/Kluwer Wireless Networks", 2011, vol. 17, n^{o} 8, p. 1775-1794.

[25] B. DONNET, B. GUEYE, M. A. KAAFAR. *Path similarity evaluation using bloom filters*, in "Computer Networks", 2011, http://dx.doi.org/10.1016/j.comnet.2011.11.003.

[26] L. A. GRIECO, C. BARAKAT, M. MARZULLI. *Spectral Models for Bitrate Measurement from Packet Sampled Traffic*, in "IEEE Transactions on Network and Service Management", June 2011, vol. 8, n^{o} 2.

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

[28] I. POESE, S. UHLIG, M. A. KAAFAR, B. DONNET, B. GUEYE. *IP Geolocation Databases: Unreliable?*, in "ACM SIGCOMM Computer Communication Review", April 2011, vol. 41, n^{o} 2.

[29] P.-U. TOURNOUX, E. LOCHIN, J. LACAN, A. BOUABDALLAH, V. ROCA. *On-the-fly erasure coding for real-time video applications*, in "IEEE Transactions on Multimedia", August 2011, vol. 13, n^{o} 4.

International Conferences with Proceedings

[30] E. ALTMAN, A. LEGOUT, Y. XU. *Network Non-Neutrality Debate: An Economic Analysis*, in "IFIP Networking 2011", Valencia, Spain, Springer, May 2011, 12, http://hal.inria.fr/inria-00568922/en.

[31] R. N. BIN RAIS, M. ABDELMOULA, T. TURLETTI, K. OBRACZKA. *Naming for Heterogeneous Networks Prone to Episodic Connectivity*, in "IEEE WCNC", Cancun, Mexico, March 2011.

[32] R. N. BIN RAIS, M. MENDONCA, T. TURLETTI, K. OBRACZKA. *Towards Truly Heterogeneous Internets: Bridging Infrastructure-based and Infrastructure -less Networks*, in "The third International Conference on COMmunication Systems and NETworkS (COMSNETS)", Bangalore, India, January 2011.

[33] E. BURSZTEIN, R. BEAUXIS, P. HRISTO, D. PERITO, C. FABRY, J. MITCHELL. *The Failure of Noise-Based Non-Continuous Audio Captchas*, in "Proceedings of the 37th IEEE Symposium on Security & Privacy", Oakland California, 2011.

[34] C. CASTELLUCCIA, G. ACS. *I have a DREAM! (DiffeRentially privatE smArt Metering)*, in "Proceedings of the The 13th Information Hiding Conference (IH)", 2011.

[35] C. CASTELLUCCIA, G. ACS, W. LECAT. *Protecting against Physical Resource Monitoring*, in "Proceedings of the 10th ACM Workshop on Privacy in the Electronic Society (WPES)", 2011.

[36] C. CASTELLUCCIA, E. DE CRISTOFARO, A. FRANCILLON, M. ALI KAAFAR. *EphPub: Toward Robust Ephemeral Publishing*, in "proceedings of the 19th IEEE International Conference on Network Protocols (ICNP)", Vancouver, October 2011, http://ephpub.googlecode.com.

[37] 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.

[38] M. JABER, R. CASCELLA, C. BARAKAT. *Boosting statistical application identification by flow correlation*, in "proceedings of EuroNF-TCCFI (International Workshop on Traffic and Congestion Control for the Future Internet)", Greece, April 2011.

[39] M. JABER, R. CASCELLA, C. BARAKAT. *Can we trust the inter-packet time for traffic classification?*, in "proceedings of IEEE International Conference on Communications (ICC)", Kyoto, Japan, June 2011.

[40] M. JABER, R. CASCELLA, C. BARAKAT. *Using host profiling to refine statistical application identification*, in "proceedings of IEEE INFOCOM Mini-Conference", Orlando, FL, March 2012.

[41] A. KRIFA, C. BARAKAT, T. SPYROPOULOS. *MobiTrade: Trading Content in Disruption Tolerant Networks*, in "proceedings of ACM Mobicom Workshop on Challenged Networks (CHANTS)", Las Vegas, September 2011.

[42] A. LABIDI, S. METTALI 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.

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

[44] I. LASSOUED, C. BARAKAT. *A Multi-task Adaptive Monitoring System Combining Different Sampling Primitives*, in "proceedings of the 23rd International Teletrafic Congress (ITC)", San Francisco, September 2011.

[45] S. LE BLOND, P. MANILS, A. CHAABANE, M. A. KAAFAR, C. CASTELLUCCIA, A. LEGOUT, W. DABBOUS. *One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users*, in "4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11)", Boston, United States, USENIX, March 2011, http://hal.inria.fr/inria-00574178/en.

[46] 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 "Internet Measurement Conference (ACM/USENIX IMC)", ACM/USENIX, November 2011, http://hal.inria.fr/inria-00632780/en.

[47] 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.

[48] A. QUEREILHAC, M. LACAGE, C. FREIRE, T. TURLETTI, W. DABBOUS. *NEPI: An Integration Framework for Network Experimentation*, in "19th International Conference on Software Telecommunications and Computer Networks (SoftCOM)", Dubrovnik, Croatia, September 2011.

[49] 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.

[50] C. TALA, L. AHUMADA, D. DUJOVNE, S. UR-REHMAN, T. TURLETTI, W. DABBOUS. *Guidelines for the accurate design of empirical studies in wireless networks*, in "7th International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom)", Shangai, China, April 2011.

[51] S. UR-REHMAN, T. TURLETTI, W. DABBOUS. *Multicast Video Streaming over WiFi Networks: Impact of Multipath Fading and Interference*, in "IEEE Workshop on multiMedia Applications over Wireless Networks (MediaWiN)", Corfu, Greece, June 2011.

[52] R. VILARDI, L. A. GRIECO, G. BOGGIA, C. BARAKAT. *Adaptation of Real-time Temporal Resolution for Bitrate Estimates in IPFIX Systems*, in "proceedings of the 2nd International Workshop on TRaffic Analysis and Classification (TRAC)", Istanbul, July 2011.

Research Reports

[53] A. KRIFA, C. BARAKAT, T. SPYROPOULOS. *MobiTrade: Interest driven content dissemination architecture for Disruption Tolerant Networks*, INRIA, February 2011, http://hal.inria.fr/inria-00568235/en.

[54] T. PAILA, R. WALSH, M. LUBY, V. ROCA, R. LEHTONEN. *FLUTE - File Delivery over Unidirectional Transport (revised)*, February 2011, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-12.txt>.

[55] S. REHMAN, T. TURLETTI, W. DABBOUS. *A Roadmap for Benchmarking in Wireless Networks*, INRIA, August 2011, n^{o} RR-7707, http://hal.inria.fr/inria-00614167/en.

[56] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, October 2011, IETF RMT Working Group (individual document), Work in Progress: <draft-ietf-rmt-newfcast-05.txt>.

[57] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, July 2011, IETF RMT Working Group (individual document), Work in Progress: <draft-ietf-rmt-newfcast-04.txt>.

[58] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, February 2011, IETF RMT Working Group (individual document), Work in Progress: <draft-ietf-rmt-newfcast-03.txt>.

[59] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Simple Reed-Solomon Forward Error Correction (FEC) Scheme for FECFRAME*, November 2011, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-simple-rs-02>.

[60] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Simple Reed-Solomon Forward Error Correction (FEC) Scheme for FECFRAME*, September 2011, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-simple-rs-01>.

[61] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Simple Reed-Solomon Forward Error Correction (FEC) Scheme for FECFRAME*, February 2011, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-simple-rs-01>.

[62] V. ROCA. *Simple Authentication Schemes for the ALC and NORM Protocols*, December 2011, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-simple-auth-for-alc-norm-06.txt>.

[63] V. ROCA. *Simple Authentication Schemes for the ALC and NORM Protocols*, September 2011, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-simple-auth-for-alc-norm-05.txt>.

[64] V. ROCA. *Simple Authentication Schemes for the ALC and NORM Protocols*, July 2011, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-simple-auth-for-alc-norm-04.txt>.

[65] 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)*, July 2011, IETF RMT Working Group, Work in Progress: <draft-roca-rmt-goe-fec-00.txt>.

[66] V. ROCA, A. ROUMY, B. SAYADI. *The Generalized Object Encoding (GOE) LDPC-Staircase FEC Scheme*, October 2011, IETF RMT Working Group, Work in Progress: <draft-roca-rmt-goe-ldpc-00.txt>.

[67] A. ROUMY, V. ROCA, B. SAYADI, R. IMAD. *Unequal Erasure Protection and Object Bundle Protection with the Generalized Object Encoding Approach*, INRIA, July 2011, n^{o} RR-7699, submitted to Infocom 2012, http://hal.inria.fr/inria-00612583/en.

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

[69] M. WATSON, A. BEGEN, V. ROCA. *Forward Error Correction (FEC) Framework*, June 2011, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-framework-15.txt>.

[70] M. WATSON, A. BEGEN, V. ROCA. *Forward Error Correction (FEC) Framework*, March 2011, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-framework-14.txt>.

[71] M. WATSON, A. BEGEN, V. ROCA. *Forward Error Correction (FEC) Framework*, February 2011, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-framework-13.txt>.

[72] M. WATSON, A. BEGEN, V. ROCA. *Forward Error Correction (FEC) Framework*, January 2011, IETF FECFRAME Working Group, Work in Progress: <draft-ietf-fecframe-framework-12.txt>.

Other Publications

[73] S. BOUCKAERT, V. VAN GERWEN, M. INGRID, S. C. PHILLIPS, J. WILANDER, S. UR-REHMAN, T. TURLETTI, W. DABBOUS. *"Benchmarking computers and computer networks"*, September 2011, Whitepaper, IST Fire projects.

[74] A. KRIFA, M. MENDONCA, R. N. B. RAIS, C. BARAKAT, T. TURLETTI, K. OBRACZKA. *"Efficient Content Dissemination in Heterogeneous Networks Prone to Episodic Connectivity"*, August 2011, Demo at ACM Sigcomm.