INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Planète

Protocols and applications for the Internet

Sophia Antipolis - Méditerranée, Grenoble - Rhône-Alpes

Theme : Networks and Telecommunications

Activity Report

2010

Table of contents

1. Team

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

Bilel Ben Romdhanne [Associate Engineer, until January 2010]
Jonathan Detchart [Associate Engineer ADT]
Giovanni Gherdovich [Expert Engineer, until December 2010]
Amir Krifa [Expert Engineer and PhD student]
Mathieu Lacage [Dream Engineer and PhD student until November 2010]
Baris Metin [Expert Engineer]
Faker Moatamri [Expert Engineer, until March 2010]
Thierry Parmentelat [Dream Engineer]
Alina Quereilhac [Associate Engineer]
Anil Kumar Vengalil [Expert Engineer, until February 2010]

PhD Students

Sana Ben Hamida [Funding CEA LETI]
Abdelberi Chaabane [Funding ANR ARESA2 contract, since September 2010]
Mathieu Cunche [Funding ANR and R&D contract, until May 2010]
Amine Ismail [Funding CIFRE Scholarship with UDcast, until June 2010]
Mohamad Jaber [Funding MESR Scholarship & ATER]
Ludovic Jacquin [Minalogic Inria grant]
Imed Lassoued [Funding ECODE project]
Stevens Le Blond [Funding Inria CORDIS Scholarship & OneLab2 contract]
Pere Manils [Finding Inria CORDIS, until November 2010]
Ferdaouss Mattoussi [Funding ADR, Alcatel Lucent contract, since February 2010]
Daniele Perito [Funding WSN4CIP IST project]
Rao Naveed Bin Rais [Funding Pakistanian Scholarship]
Ashwin Satish Rao [Funding OneLab2 and Connect projects]
Mohamed Karim Sbai [Funding ITEA ExpeShare project, until September 2010]
Shafqat Ur-Rehman [Funding OneLab2 and F-Lab projects]

Post-Doctoral Fellows

Roberto Cascella [Funding CMON project]
Mate Soos [Funding Inria grant, until November 2010]
Rodrigue Imad [Funding ADR, Alcatel Lucent contract, since October 2010]
Gergely Acs [Funding Inria CORDIS, since May 2010]

Visiting Scientists

Kazuhisa Matsuzono [Visiting PhD from Keio, from February to March 2010]
Marc Mendonca [Visiting Master from UCSC, March 2010]
Amine Elabidi [Visiting PhD from ENSI Tunis, July - August and October - November 2010]

Administrative Assistants

Dominique Guédon [until november 2010]
Anais Cassino [since december 2010]
Helen Pouchot [Grenoble]

Others

Mariem Abdelmoula [Ubinet Intern, from March to August 2010]
Chérifa Boucetta [ENSI Intern, from February to June 2010]
Aldelberi Chaabane [ENSI Intern, from October 2009 to March 2010]
Ilias Chatzidrosos [KTH PhD Intern, from April to July 2010]
Carlo D'Elia [Politecnico di Bari PhD Intern, from March to July 2010]
Nabil Echaouch [ENSI Intern, from February to June 2010 and from September 2010]
Saghar Estehghari [UCL, from January 2010]
Martin Ferrari [Ubinet Intern, from April to September 2010]
Kamel Trimeche [ENSI Intern, from February to June 2010]

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 protocol 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 (UCI, UCLA, UCSC, U. Arizona, U. Lancaster, Princeton U., U. Washington, U. Berne, EPFL, U. Pisa, RPI, LIP6, Eurecom, etc.) and industrial (Ericsson, Nokia, SUN, Docomo, Expway, Hitachi, Alcatel, FT R&D, LGE, STMicroelectronics, Motorola, Intel, Netcelo, NEC, Boeing, etc.) partners.

2.2. Highlights

- Our research activities received a lot of media attention this year (several articles in US newspapers, MIT TechReview, Slashdot, Registers, ACM news, International general audience press...).
- Signature of the ns-3 consortium in July 2010. See the new results section.

3. Scientific Foundations

3.1. Networking Experimentation

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 see Figure 1). 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 network simulators and experimental platforms (see Figure 2). We work in close collaboration with research and development industrial teams.

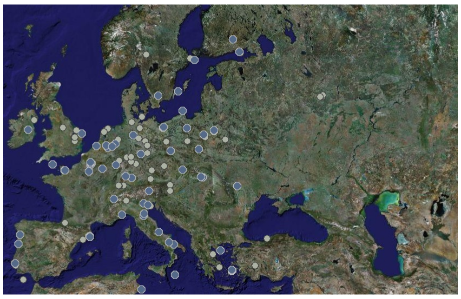

Figure 1. PlanetLab Europe Experimental Network

Figure 2. Wireless Experimentation Network at INRIA Sophia Antipolis

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. Applications domains

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 oue 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 trace-route, but they are unable to provide detailed answers on the source of the problem nor on its location. From operator point of view, the situation is not better since an operator has only access to its own network and can hardly translate local information into end-to-end measurements. The increase in the complexity of networks as is the case of wireless mesh networks will not ease the life of users and operators. The purpose of our work in this direction 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 unified 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.

The evaluation of new network protocols and architectures is at the core of networking research. This evaluation is usually performed using simulations (e.g., NS), emulations (e.g., Emulab), or in the wild experimental platforms (e.g., PlanetLab). 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 in 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: Mathieu Lacage [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 ip/tcp 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. EphCom

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

EphCOM (Practical Ephemeral Communications) implements a novel key storage mechanism for disappearing data systems, that relies on the caching mechanism of the Domain Name System. Features of EphCOM include: EphCOM exploits the fact that DNS servers temporarily cache the response to a recursive DNS query for potential further requests. EphCOM provides higher security than Vanish, as it is immune to Sybil attacks. EphCOM is easily deployable and does not require any additional infrastructure, such as Distributed Hash Tables. EphCOM comes with high usability as it does not require users to install and execute any extra additional software. EphCOM lets users define data lifetime with high granularity.

See also the web page http://code.google.com/p/disappearingdata/.

- 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. NEPI

Participants: Mathieu Lacage [correspondant], Alina Quereilhac, Martin Ferrari.

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.
See also the web page http://yans.pl.sophia.inria.fr/trac/nepi.

- 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

5.4. SFA Federation of PlanetLab networks

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

In the context of the OneLab project, we are in charge of the development activities for the PlanetLab Europe platform, which uses the mainstream PlanetLab software codebase that turns out to be a codevelopment effort between our project-team and Princeton University. A major contribution has been to write the first implementation of the federation mechanism that allows PlanetLab Central and PlanetLab Europe to run as peer systems, offering to any user a consolidated view of all federating resources regardless of the user's affiliation. We have also contributed various improvements to handle more heterogeneous types of hardware, like e.g. wireless or multi-homed connectivity. The codevelopment model takes advantage of the decentralized source control tool *git*. The software built out of our codebase is known as 'the OneLab build' of the PlanetLab software. We know of at least two institutions, HUJI and University of Tokyo, who use this release rather than the Princeton one. The builds that are published for PlanetLab Europe, and for the general public, can be found under http://build.onelab.eu/, now differ from the stock PlanetLab distribution only by a few tweaks.

During 2010, we have kept on developping new features and enhancements for the PlanetLab software. A substantial part of our activities has been devoted to the new federation architecture known as SFA, that was designed as a side-effect of the NSF GENI Project by a joint effort across several testbed software flavours, including PlanetLab and Emulab. We have contributed to the development of the PlanetLab implementation of SFA, have implemented validation tools for releasing these, and have played a crucial role in the roll out of SFA at a real scale between PlanetLab Central, PlanetLab Europe, PlanetLab Japan, and PPK in Korea. Also worth being noted, this embryo of a federation just reached the Emulab world, meaning that we can start using SFA to provision experiment across testbeds, i.e. involving resources that span PlanetLab and/or Emulab resources, although this is still quite experimental as of yet. Finally, we have also written a user-tool for SFA known as *sface*.

In addition to this we have issued a few releases of *MyPLC*, including (*) the integration of the OMF experimental plane, that lets a user manage an experiment on resources from ORBIT-like testbeds and/or from a PlanetLab testbed in a unified way, (*) a new User Interface known as *MySlice* for much easier resource selection, (*) a reworked tag permission system, (*) support for recent distributions (fedora12, fedora14 is alpha, centos6 is expected for 2011), and (*) for more recent kernels (2.6.32 is beta).

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

- Version: myplc-5.0-rc17
- Keywords: networking testbed virtual machines
- License: Various Open Source Licences
- Type of human computer interaction: Web-UI, XMLRPC-based API
- OS/Middelware: Linux-Fedora
- Required library or software: Fedora-12 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

5.5. 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.

5.6. LDPC large block FEC codec

Participant: Vincent Roca [correspondant].

We developed a large block LDPC (Low-Density Parity-Check) codec. Our codec is the only Open-Source, patent free, large block FEC (Forward Error Correction) codec for the Packet Erasure Channel (e.g. Internet) available today. It is both integrated in our MCLv3 library and distributed independently in order to be used by third parties in their own applications or libraries. This software, which is unique in the world, has experienced a lot of interest in both academic and industrial environments. In particular, this work has been largely supported by STmicroelectronics and the LDPC FEC codes are currently being considered for possible standardization in the IETF and DVB-H/SH organizations. See http://planete-bcast.inrialpes.fr/ for more information.

5.7. BitHoc

Participants: Chadi Barakat [correspondant], Thierry Turletti, Mohamed Karim Sbai, 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

5.8. TICP

Participants: Chadi Barakat [correspondant], Mohamed Karim Sbai.

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

5.9. 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.

CrunchXML

CrunchXML is part of the Wireless Experimentation (WEX) toolbox, 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 packet fields that have been marked as relevant by the user in a MySQL database –original pcap traces should be first formated 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.

6. New Results

6.1. Towards Data-Centric Networking

Participants: Rao Naveed Bin Rais, Chadi Barakat, Mathieu Cunche, Walid Dabbous, Jonathan Detchart, Amine Ismail, Rodrigue Imad, Mohamed Ali Kaafar, Amir Krifa, Mathieu Lacage, Ferdaouss Mattoussi, Vincent Roca, Mohamed Karim Sbai, Thierry Turletti.

- **Disruption Tolerant Networking**

  Communication networks are traditionally assumed to be connected. However, emerging wireless applications such as vehicular networks, pocket-switched networks, etc. coupled with volatile links, node mobility, and power outages, will require the network to operate despite frequent disconnections. To this end, opportunistic routing techniques have been proposed, where a node may store-and-carry a message for some time, until a new forwarding opportunity arises. Although a number of such algorithms exist, most focus on relatively homogeneous settings of nodes. However, in many envisioned applications, participating nodes might include handhelds, vehicles, sensors, etc. These various classes have diverse characteristics and mobility patterns, and will contribute quite differently to the routing process. In [34], [9] we have analyzed existing opportunistic routing strategies into a small number of common and tunable routing modules (e.g. message replication, coding, etc.), in order to identify how and when a given routing module should be used, depending on the set of network characteristics exhibited by the wireless application. We then proposed a taxonomy for intermittently connected networks. We identified generic network characteristics that are relevant to the routing process (e.g., network density, node heterogeneity, mobility patterns) and dissect different challenged wireless networks or applications based on these characteristics. The objective of this study was to identify a set of useful design guidelines that will enable one to choose an appropriate routing protocol for the application or network in hand.

  In the same research area, we have designed an efficient message delivery mechanism, called MeDeHa, which enables distribution/dissemination of messages in an Internet connecting heterogeneous networks and prone to disruptions in connectivity [36]. MeDeHa is complementary to the IRTF's Bundle Architecture: while the Bundle Architecture provides storage above the transport layer in order to enable interoperability among networks that support different types of transport protocols, MeDeHa is able to store data at any layer of the network stack, addressing heterogeneity even at lower layers (e.g., when intermediate nodes do not support higher-layer protocols). It also takes advantage of network heterogeneity (e.g., nodes supporting more than one network and nodes having diverse resources) to improve message delivery. For example, in the case of IEEE 802.11 networks, participating nodes may use both infrastructure- and ad hoc modes to deliver data to otherwise unavailable destinations. Another important feature of MeDeHa is that it does not rely on special-purpose nodes such as message ferries, data mules, or throwboxes in order to relay data to intended destinations, and/or to connect to the backbone network wherever infrastructure is available. The network is able to store data destined to temporarily unavailable nodes for some time depending upon current storage availability as well as quality-of-service needs (e.g., delivery delay bounds) imposed by the application. We showcased MeDeHa's ability to operate in environments consisting of a diverse set of interconnected networks and evaluated its performance via extensive simulations using a variety of synthetic and more realistic scenarios. Our results show significant improvement in average delivery ratio and significant decrease in average delivery delay in the face of episodic connectivity.

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. However, to date there are no comprehensive solutions that integrate MANETs to infrastructure-based networks. We have extended the MeDeHa framework to bridge together infrastructure-based and infrastructure-less networks [13]. Through extensive simulations, we demonstrated the benefits of the new framework, 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 to conduct experiments in "hybrid" scenarios running partly on simulation and partly on real nodes [55], [54].

These different works are the result of collaborations with Thrasyvoulos Spyropoulos from ETH Zurich, Katia Obraczka and Marc Mendonca from University of California Santa Cruz (UCSC). They are done in the context of the COMMUNITY INRIA Associated Team, see 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. Therefore, in order to achieve data delivery in such challenging environments, researchers have proposed the use of store-carry-and-forward protocols: 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 proposed 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 derive an optimal policy using global knowledge about the network, then we introduce a distributed algorithm that collects statistics about network history and uses appropriate estimators for the global knowledge required by the optimal policy. 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 previous works. 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/).

- **File Sharing in Wireless Ad Hoc Networks**

  This activity started with the PURPURA COLOR projet in conjunction with the LIA laboratory at the University of Avignon and grows within the ExpeShare ITEA European project. The latter project started in February 2007 and ended in October 2009. Within this activity, we focus on file sharing over wireless ad hoc networks. File sharing protocols, typically BitTorrent, are known to perform very well over the wired Internet where end-to-end performances are almost guaranteed. However, in wireless ad-hoc networks the situation is different due to topology constraints and the fact that nodes are at the same time peers and routers. For example, in a wireless ad-hoc network running standard BitTorrent, sending pieces to distant peers incurs lots of overhead due to resources consumed in intermediate nodes. Moreover, TCP performance is known to drop seriously with the number of hops. Running file sharing with its default configuration no longer guarantees the best performances. For instance, the neighbor and piece selection algorithms in BitTorrent need to be studied in the wireless ad-hoc scenarios, since it is no longer efficient to choose and treat with peers independently of their location. A potential solution could be to limit the scope of the neighborhood. In this case, TCP connections are fast but pieces will very likely propagate in a unique direction from the seed to distant peers. This would prohibit peers from reciprocating data and would result in low sharing ratios and suboptimal utilization of network resources. There is a need for a solution that minimizes the average download finish time per peer while encouraging peers to collaborate by enforcing a fair sharing of data.

  Within this activity, we present a solution to the aforementioned problem and we validate it by simulations and extensive experiments over the well known ORBIT platform (Rutgers ORBIT project team http://www.orbit-lab.org), for instance see [30] for details. This solution has been the main contribution of the PhD thesis of Mohamed Karim Sbai, who graduated in October 2010 [4]. It takes into consideration the limitations of wireless networks and aims to minimize the global download time of users by decreasing the network load and ensuring fair cooperation among peers. For this, it adapts the algorithms of BitTorrent, mainly the neighborhood selection algorithm to the topology of the wireless network, the mobility of nodes and the cross traffic. In addition to considering the data plane, it also integrates algorithms to discover and update the members of a P2P overlay in mobile wireless networks. The latter algorithms adapt to arrivals and departures of peers and changes in the topology due to the mobility of nodes. The objective is to minimize the membership traffic while keeping a good freshness of the information about the members.

  To push our research further in this direction and to give it a practical flavor, we have worked on the design and implementation of a new application that enables content sharing among spontaneous communities of mobile users using wireless multi-hop connections. Our application is called BitHoc, which stands for BitTorrent for wireless ad hoc networks. It is an open source software developed under the GPLv3 licence. BitHoc is made public and is available for download at this URL http://planete.inria.fr/bithoc. It includes two principal components: a membership management service and a content sharing service. As classical tracker-based BitTorrent membership management and peer discovery are unfeasible in ad hoc networks, we design the membership management service as a distributed tracker overlay that connects peers involved in the same sharing session. Using the membership information provided by the tracker overlay, the content sharing service schedules the data transfer connections among the session members by leveraging the multi-hop routing feature of wireless ad-hoc networks. The testbed in its current form is composed of PDAs and smartphones equipped with WIFI adapters and Windows Mobile 6 operating system.

- **Optimizing the DVB-SH FEC Scheme for Efficient Erasure Recovery**

  Protection of data against long fading time is one of the greatest challenges posed by a satellite delivery system offering multimedia services to mobile devices like DVB-SH (Digital Video Broadcast - Satellite services to Handhelds). To deal with this challenge, several enhancements and modifications of the existing terrestrial mobile TV (DVB-H) are being considered. These solutions provide the required protection depth but they don't take into account the specificity of mobile handheld devices such as power consumption, memory constraints and chipsets implementation costs. We proposed an innovative algorithm (called Multi Burst Sliding Encoding or MBSE) that extends the DVB-H intra-burst (MPE-FEC) protection to an inter-burst protection so that complete burst losses could be recovered while taking into account the specificity of mobile handheld devices. Based on a clever organisation of the data, our algorithm provides protection against long term fading while still using RS code implemented in DVB-H chipsets. We evaluated the performance of MBSE by both theoretical analysis as well as intensive simulations and experiments. The results also show good performance in terms of protection, battery and memory saving. The MBSE was standardised by the DVB Forum as the main solution for the DVB-SH class terminals. We proposed also a method to optimize the MBSE parameters and an analysis of the performance gain. Various sets of parameters are studied and optimized with respect to the link performance. Furthermore, we have designed an algorithm to compute the optimum values of the MBSE parameters according to some constraints. We have implemented MBSE in two UDcast DVB-SH equipments and have validated the optimization method using intensive experiments with typical usage scenarios under a hardware-emulated wireless link. This activity had industrial impact as it was implemented in UDcast commercial equipment. In addition, the algorithm was standardized by the DVB-SH forum as MPE-iFEC (Multi-Protocol Encapsulation - inter-burst Forward Error Correction). The DVB forum had identified the need for a MAC layer protection scheme for multimedia flows in satellite to handheld devices communications. Physical layer protection represented a technical problem (for chip manufacturers) and commercial problem for telephone vendors. Several solutions were discussed at the DVB forum among them: MBSE, Raptor codes proposed by Digital Fountain Inc and LDPC codes. Among the two solutions that were selected (MBSE and Raptor), ours had a shorter time to market because it reuses the RS codecs already available in DVB-H circuits. Therefore the MBSE sliding encoding was adopted and renamed MPE- iFEC by the DVB forum as the standard solution for "class A" terminals.

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

  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).

  After the publication of RFC 5170 in 2008, our specification of Reed-Solomon codes and their use has been published in 2009 in RFC 5510 ("proposed standard" maturity level). We also performed a detailed performance comparison of LDPC-Staircase, Reed-Solomon and Raptor codes in a paper published in CFIP'09. We also studied the possibility of light-weight software decoding of Reed-Solomon codes.

  Another activity consisted in improving the decoding of AL-FEC codes thanks to an appropriate code structure. Indeed, the ML (Maximum Likelihood) decoding of LDPC codes (e.g. as specified in RFC 5170) is sooner or later limited by Gaussian pivoting algorithmic complexity. The idea is therefore to design LDPC codes that, thanks to their inner structure, feature at the same time good erasure recovery capabilities and high speed decoding under both iterative decoding and ML decoding. This work has been published in Globecom'09 and in [19]. Banded Quasi-cyclic LDPC codes in particular may be a promising solution for a new generation of high performance LDPC codes.

  We have also studied an extension of LDPC-Staircase codes in order to provide an object-level authentication service. The system designed, called VeriFEC, enables a receiver to identify the vast majority of corrupted objects (the detection probability amounts to 99.86% in case of a single random symbol corruption) almost for free. This work has been published in Globecom'09.

- **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. 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: [37], [38], [49], [47], [48], [46], [50].

In parallel we have started an implementation of the FECFRAME framework in order to gain an in-depth understanding of the system. The results [28] show the benefits of LDPC-Staircase codes when dealing with high bit-rate real-time flows.

In the context of robust streaming systems, we also contributed to the analysis of the Tetrys approach, in [57], [56]. 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 [45], [44].

- **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: [51].

  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 [52]. This activity is also carried out within the IETF RMT working group.

- **Authorization Management in Grids**

  This work, carried out as part of the HIPCAL project, proposes to combine the network and system virtualization with the SPKI/HIP/IPsec protocols, in order to help the Grid communities to build and share their own computing intensive systems. More specifically, the security and authorization management system relies on the Simple Public Key Infrastructure (SPKI) protocol, which enables the creation of a lightweight, dynamic and extensible, private authorization management system, that is in line with the requirements of Grid systems.

  We have implemented a SPKI library, with an API that enables its use in the context of HIPCAL but also in other use-cases. An in-depth analysis and performance evaluation is currently under progress.

- **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 the feasibility of high-bandwidth, secure communications on generic machines equipped with the latest CPUs and General-Purpose Graphical Processing Units (GPGPU). This work has been published in [23].

6.2. Network Security and Privacy

Participants: Sana Ben Hamida, Claude Castelluccia, Abdelberi Chaabane, Walid Dabbous, Mohamed Ali Kaafar, Arnaud Legout, Stevens Le Blond, Pere Manils, Daniele Perito, Mate Soos.

- **Information Leakage in Web Services**

  The amount of personal information stored at remote service providers increases, so does the danger of private information leakage. In this work, we studied privacy leakages related to Google services, and more specifically Google Web History. This service records all searches made by a Google signed-in user. The Web History is used to provide personalized results and keyword suggestions for searches that a user has already made. We designed the Historiographer, a novel inference attack that reconstructs the web search history of Google users, even though this service is supposedly protected from session hijacking by a stricter access control policy. The Historiographer uses a reconstruction technique to infer search history from the personalized suggestions fed by the Google search engine. Its validity is confirmed through experiments conducted over real network traffic. We point out th at our attacks are general, not specific to Google.

  This result was published at PETS'2010, one of the most prestigious conference in the area of Computer Privacy. This work received a lot of media attention (several articles in US newspap ers, MIT TechReview, Slashdot, Registers, ACM news,...). See http://planete.inrialpes.fr/projects/private-information-disclosure-from-web-searches/ for more details.

- **Architecture of Privacy**

  We had several other significant contributions in the area of Internet Privacy. For example, we designed several attacks against the TOR network (an anonymization network). We showed that the IP addresses of BitTorrent users on top of Tor can easily be identified. This results had a great impact and visibility within and outside the research community. We also worked on the problem of the "droit à l'oubli". The increasing amount of personal information disseminated over the Internet raises serious privacy concerns. Data may linger forever, and users often lose its control and ownership. This motivates the desire of binding availability of contents to expiration times set by the data owner. To this end, we formalized the notion of Ephemeral Data Systems (EDSs): EDSs protect privacy of past data and prevent malicious parties from accessing expired contents. We designed EphCom, a practical EDS using only a primary Internet service — the Domain Name Service (DNS) and its caching mechanism. EphCom does not rely on Trusted Platform Modules (TPM), centralized servers, peer-to-peer networks, or proactive actions of the users. It is transparent to existing applications and services, and allows users to tightly control data lifetime. We developed Firefox extension that provides ephemeral email capabilities and a command line tool for ephemeral files. The TOR attacks were published at HotPETS'2010, and received impressing media attention (with a countless number of articles). A prototype of EphCOM has been implemented and distributed on the Web.

- **Physical Security**

  Recent security methods propose to generate secret keys from Ultra Wide Band (UWB) channels. These solutions rely on the reciprocity and spatial channel correlation p rinciples. This project aims to present empirical studies on the aforesaid properties. First, we verified the UWB reciprocity for different scenarios (LOS, nLOS). We showed, experimentally, that the reciprocity is always valid independently of distance between the receiver and emitter. However, the use of an asymmetric hardware in up and down links, can affect the channel similarity. We also performed measurements of spatial correlation in near and far field channel. Various experimental scenarios were tested to validate location channel variations. We observed that in very close and far receiver's locations, there is no correlation. This variation depends mainly on the number of clutters in the indoor environment. In addition, various channel parameters (channel impulse response "CIR", channel envelope, and power delay profile "PDP") have been investigated. We showed that channel properties depend on these parameters.

- **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 [27], [39] and received a very large media coverage (see http://www-sop.inria.fr/members/Arnaud.Legout/Projects/bluebear.html) .

  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. However, we showed in a second study that it is possible to retrieve the IP address for more than 70% of BitTorrent users on top of TOR [31]. 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.

- **Secure Localization in Wireless Sensor Networks**

  Remote monitoring and gathering information are the main objectives behind deploying Wireless Sensor Networks (WSNs). Besides WSN issues due to communication and computation restricted resources (low energy, limited memory computational speed and bandwidth), securing sensor networks is one of the major challenges these networks have to face. In particular, the security of sensors localization is a fundamental building block for many applications such as efficient routing. In this work, we introduce a new threat model that combines classical Wormhole attacks (i.e. an attacker receives packets at one location in the network, tunnels and replays them at another remote location using a powerful transceiver as an out of band channel) with false neighborhood topology information sent by the wormhole endpoints themselves or by some colluding compromised nodes.

We show using intensive simulations how this clever attacker that would exploit the neighborhood topology information can easily defeat two representative secure localization schemes. We also propose some possible countermeasures and evaluate the first corresponding results. This work has been published in ICST S-cube 2010 [14].

- **Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network**

  Users' anonymity and privacy are among the major concerns of today's Internet. Anonymizing networks are then poised to become an important service to support anonymousdriven Internet communications and consequently enhance users' privacy protection. Indeed, Tor an example of anonymizing networks based on onion routing concept attracts more and more volunteers, and is now popular among dozens of thousands of Internet users. Surprisingly, very few researches shed light on such an anonymizing network. Beyond providing global statistics on the typical usage of Tor in the wild, we show that Tor is actually being mis-used, as most of the observed traffic belongs to P2P applications. In particular, we quantify the BitTorrent's traffic and show that the load of the latter on the Tor network is underestimated because of encrypted BitTorrent traffic (that can go unnoticed). Furthermore, this work provides a deep analysis of both the HTTP and BitTorrent protocols giving a complete overview of their usage. We do not only report such usage in terms of traffic size and number of connections but also depict how users behave on top of Tor. We also show that Tor usage is now diverted from the onion routing concept and that Tor exit nodes are frequently used as 1-hop SOCKS proxies, through a so-called tunneling technique. We provide an efficient method allowing an exit node to detect such an abnormal usage. Finally, we report our experience in effectively crawling bridge nodes, supposedly revealed sparingly in Tor. This work has been published in IEEE NSS 2010.

- **Monitoring privacy threats in current OSNs' applications.**

  Buzz, the new Online Social Networking (OSN) service from Google has been introduced recently. Even though it raised big concerns (and even complaints) about several privacy issues, Buzz has been already launched inside millions of Gmail accounts. In this paper, we show that one of the major concerns Buzz might have to deal with is that it is integrated into the Google email service. In fact, to use Buzz one has to sign up for a Google profile that will primarily be seen by other Google users. However this profile, as shown in this paper reveals for the vast majority of Buzz users their Gmail usernames, and so their Google email addresses. We exploit the notion of Followers/Follwing in Buzz to crawl Google for Gmail accounts, demonstrating how it is easy and practical to collect millions of valid Gmail accounts from a single machine, in a very short period of time and without being noticed. The collected email addresses have many desirable properties from a spammer's perspective. They are valid email addresses, that refer to active and individual Buzz users that participate in online social activities, increasing then the efficiency of spam campaigns targeting these users. We then show how spammers can even use the Google infrastructure to categorize the email accounts they collected based on specific area of interest of users. As a conclusion, we demonstrate that integrating Buzz to email accounts, and hence to Google profiles offers spammers with a valuable, yet not risky, way to build a giant Google emails-made spammer database. This work has been published in EuroSYS SNS 2010 [24].

6.3. Network Monitoring

Participants: Chadi Barakat, Roberto Cascella, Amir Krifa, Imed Lassoued, Mohamad Jaber, Mohamed Karim Sbai.

The main objective of our work in this domain is a better monitoring of the Internet and a better control of its resources. In the monitoring part, we work on new measurement techniques that scale with the growth of the Internet size and fast increase in the traffic. We propose solutions for a fast and accurate identification of Internet traffic based on packet size statistics. 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. 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. In the network control part, we focus on new solutions that improve the quality of service for users by a better management of network resources and by a more efficient tuning of applications that take into account the constraints imposed by the network. In this direction we propose distributed topology-aware algorithms for the scheduling of communications among members of a wireless community interested in sharing data files among each other and connected together in a way to form a MANET (Mobile Ad Hoc Network). We also works towards optimal algorithms for the management of storage resources and for the scheduling of communications among wireless devices that meet occasionally and that relay contents to each other in the hope to provide a global communication service. This later framework is often referred to as Delay Tolerant Networks (DTNs).

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 and the times between 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.

- **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 for 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 traffic 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 [26]. Their performances are being validated in typical scenarios over an experimental platform we developed for the purpose of the study [25]. Our platform is called MonLab (Monitoring Lab) and is described with more details in the Section on produced software. 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 whole 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 - Sep. 2011).

- **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 [20]. 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 called 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 achieves 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. These results together with the motivation for the work and the details of the approach are described in [15]. 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.

- **Exploiting Network Coordinate Systems for Monitoring**

  On another track, we work on the exploitation of virtual coordinates for network monitoring. A coordinate system embeds network delays into an Euclidean space and that associates to each machine a coordinate vector that respects its delay distances with respect to the other machines. Our objective is first to study how these coordinates evolve in reality and in normal situations, then second to develop algorithms that allow the detection of any change in the normal behavior of these coordinates and to invert this change in order to understand the origin of the problem, its location and the impacted machines. This work fits within the framework of the ANR CMON project and is an ongoing work. As a first step, we have studied the dynamics of Vivaldi coordinates in normal network conditions and have published the results of the study in [22]. The Vivaldi system is known to be one of the most interesting approaches for the calculation of Internet coordinates. It is a fully distributed, light-weight and adaptive algorithm. Recent studies show that host coordinates in the Vivaldi system are not stable and are drifting rapidly even when the network delays do not change. In this study we observe that, despite the instability of Vivaldi coordinates in their absolute values, there is still a stable internal structure that can better reflect the stability of the underlying network. We proceed for this study by extensive simulations and experimentations. In a first stage, we confirm the fact that Vivaldi coordinates oscillate over time because of the adaptive nature of the system. However the variations of these coordinates are most of the time correlated with one another pointing to a stable cluster of nodes seen from inside the network. In a second stage, we present a new clustering algorithm based on the data mining Hierarchical Grouping Method to identify this cluster of stable nodes once the network and the host coordinates reach their stationary regime. The metric that we use to cluster nodes in the system is the amount of variation of their Euclidean distances. Our main finding is that such stable cluster of nodes always exists and is grouping most of the nodes. We highlight the utility of such finding with an application that tracks changes in network delays. To this end, we propose to track a simple signal, which is the size of this biggest stable cluster.

6.4. Experimental Environment for Future Internet Architecture

Participants: Walid Dabbous, Martin Ferrari, Amine Ismail, Mathieu Lacage, Thierry Parmentelat, Alina Quereilhac, Shafqat Ur-Rehman, Thierry Turletti.

- **Enhancing Network Simulations**

  We have contributed actively to the ns-3 project since its very early stages (2006). By that time, there was a general feeling in the community that simulators are not adequate tools to validate new protocols any more. Our strategy was therefore to enhance simulations on several aspects so that they become more realistic, and easy to interface with real platforms as this would position the simulations again as a major tool in the overall validation process. The difficulties we have overcome here are manyfold: first, we had to make sure that ns-3 could receive and send real network packets with minimal CPU and memory overhead and that it could do this transparently for model developers to allow any simulation model to be used as a real-time link or network emulator interconnected with a real-world experiment. Then, we had to provide a Direct Code Execution framework for ns-3 which would allow the efficient simulation of unmodified user space and kernel space protocol implementations, hence paving the way to using the same protocol implementation during simulations and during deployments. This DCE environment is the first tool we are aware of which is able to efficiently (CPU and memory wise) reuse unmodified program binaries within a simulator. Finally, to automate the deployment of experiments comprised of simulated and real networks, we designed an object model, which is sufficiently generic to allow the description of a simulation, a testbed experiment, or a mix of these, and sufficiently flexible to allow detailed control over each experimentation tool.

  This work was done in the context of Mathieu Lacage PhD thesis defended this year with the following contributions. First, we have implemented the core facilities needed to make ns-3 the first network simulator to support transparently and efficiently the automatic conversion of network packets to and from simulation objects, hence enabling transparent support for real-time simulation in every ns-3 model. Second, we have designed a flexible unified experiment description model that is the key to allow the automated setup and deployment of mixed experiments that involve a real-time simulation, a testbed, and a field experiment. Third, we have radically extended the scope of the emulation tools' capabilities by integrating within ns-3 a Direct Code Execution (DCE) framework that encompasses both user space and kernel space protocol implementations written in C or C++ for Linux. Contrary to previous work, our solution is highly efficient and extremely robust, as it is able to deal with arbitrary protocol constructs. See [3] for more details.

  On the other hand, IEEE 802.16 WiMAX is an interesting wireless technology for providing broadband ubiquitous network access. As more and more researchers and industrials are interested in simulating such networks, a number of WiMAX simulators have been emerged in the networking community. We have implemented an IEEE 802.16 WiMAX module for the ns-3 simulator. The aim is to provide a standard-compliant and well-designed implementation of this standard. Our module implements the MAC Common-Part Sublayer (CPS), a realistic and scalable OFDM physical model, an IP packet classifier for the convergence sub-layer, efficient uplink and downlink schedulers, support for multicast traffic and pcap packet tracing functionality. The IP classifier has enabled the simulation of an unlimited number of service flows per subscriber station, while the proposed schedulers improve the management of the QoS requirements for the different service flows. The simulation module is described in [21]. Part of this work has been done in collaboration with Luigi Alfredo Grieco and Giuseppe Piro from Politecnico di Bari.

- **The ns-3 consortium**

  We have founded this year a consortium between INRIA and University of Washington. The goals of this consortium is 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 currently under reconstruction and a specific part dedicated to the consortium will be included. Georgia Tech and Bucknell University have already been invited to join the consortium as executive members. It is expected that several industrial and academic partners join the consortium in the next months.

- **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 [7]. The development of NEPI started last year 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. This 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. We plan to continue by the addition of a planetlab backend and the stabilization of the graphical user interface.

- **Taxonomy of IEEE 802.11 Wireless Parameters and Open Source Measurement Tools**

  The analysis and evaluation of new wireless network protocols is a long process that requires mathematical analysis, simulations, and increasingly experimentations under real conditions. Measurements are essential to analyze the performance of wireless protocols such as IEEE 802.11 networks in real environments, but experimentations are complex to perform and analyze. Usually, network researchers develop their own tools, sometimes from scratch, to fit the requirements of their experimentations, and these tools are then abandoned when the paper is published. We have done a survey of IEEE 802.11 wireless parameters and open source tools available to collect or estimate these parameters. In this survey, we highlighted the parameters that can be extracted from wireless traffic probes and those that are available through the driver of wireless cards. Then, we introduced and compared open source tools that can be used to make the measurements, with special attention to the flexibility of the tools and their application scope. Finally, we discussed with several case studies the combination of tools that best suit the needs of the wireless experiments and provided a list of common pitfalls to avoid [6].

- **Making easier Experimentation**

  Evaluation of network protocols and architectures are at the core of research and can be performed using simulations, emulations, or experimental platforms. 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. Experimentations allow more realistic environment and implementations, but they lack reproducibility and are complex to perform. Wireless experimentations are even more 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.

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 works on the study and optimization of various AL-FEC schemes in the context of DVB-SH or similar environments.

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.

UDcast, Sophia Antipolis: (2007-2010)

UDcast is providing a PhD grant (CIFRE contract) to support the activity on DVB-SH FEC Scheme for Efficient Erasure Recovery. This grant supported Amine Ismail who defended his PhD in June this year.

8. Other Grants and Activities

8.1. Regional Initiatives

CPER Plexus (2007-2010) :

This project aims to build an experimental wireless networking platform in several sites in Sophia Antipolis. This platform will be interconnected with the European OneLab platform through INRIA and will integrate Eurecom's radio platform. The goal is to study the performance in terms of bandwidth and radio resources utilization in a heterogeneous radio environment.

- ADT PLECS: This project (2008-2011) aims at deploying at INRIA Sophia Antipolis center a platform for networking experimentation and simulation open to regional researchers and industrials. Two Dream engineers and one Associate Engineer were attributed to our project-team by INRIA on this project.

- INRIA Grant (Ingénieur Jeune Diplômé, IJD)] (2009-2011): The goal is to design an open-source AL-FEC library.

8.2. National Initiatives

PFT (2011-2014):
DGCIS funded project, in the context of the competitive cluster SCS, whose aim is to provide to 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, Altran Méditerranée, Demtech, Ericsson, Eurécom, IQsim, MobiSmart, Monaco Télécom, Newsteo, Orange Labs, SAP, STEricsson, Telecom Valley and UDcast. Our contribution is centred on providing a test methodology and tools for wireless networks experimentation.

ANR/VERSO F-Lab (2010-2013):
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/VERSO Connect (2011-2012):
ANR funded project on content centric Networking architecture. The aim is to propose adequate naming, routing, and cache management and transmission control schemes for CCN based networks. Our contribution is centred on the design and evaluation of a personal data management system on top of CCN and on the integration of the CCNx code in the NS-3 simulator. Other partners: UPMC, A-LBLF, Orange, IT, INRIA RAP.

ANR ARESA2 (2009-2012): The Planete 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 (Planéte), Université de Savoie, and ICT/CAS (China).

RNRT RFID-AP (2008-2010):
The Planète group is involved in the RFIDAP RNRT project which aims at designing and prototyping cryptographic algorithms and secure protocols for RFID deployment. Such algorithms and protocols could be used individually, or in combination, and will provide a practical and useful framework within which to apply innovative but practical techniques for device authentication and user privacy.

FUI/SHIVA Minalogic (2009-2012):
The goal of the SHIVA (Secured Hardware Immune Versatile Architecture) project is to design a multi-Gbps security platform, compatible with high assurance environments where a clear separation between red and black flows is a must. The partners are CS (leader), EASII IC, INRIA, NETHEOS, UJF-IF, UJF-LJK, UJF-Verimag, TIMA, and IWALL.

ANR/VERSO ARSSO (2010-2013):
The goal of this project is to design adaptable robust streaming solutions. The partners include ALU-BL (leader), INRIA, CEA-LETI, ENSICA and Thales.

ANR/RNRT CAPRI-FEC (2007-2010):
The goal of this project is to design and analyze Application-Level FEC (AL-FEC) codes for the erasure channel, and their adequacy to wireless applications. The partners include INRIA (leader), CEA-LETI, ENSICA and STMicroelectronics.

ANR/CIS HIPCAL (2007-2010):

The goal of this project is to design a middle-ware that provides secure communications and assured performances to grids. This middle-ware relies on the HIP (Host Identity Protocol) subsystem, and on host virtualization techniques to dynamically define virtual, confined clusters. The middle-ware will be tested with several biomedical and bio-informatics applications. The partners are INRIA Reso (leader), INRIA Grand Large, INRIA Planète, CNRS IBCP, CNRS I3S.

INRIA Grant (Ingénieur Jeune Diplômé, IJD) (2009-2011):

The goal is to design an open-source AL-FEC library.

RNRT CMON (2009-2012) (URL http://wiki.grenouille.com/index.php/CMON):

The Planète group is a member of the CMON RNRT project which started in February 2009 and which involves, in addition to INRIA, Thomson 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 ISPs 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.

Within the CMON consortium, the Planète group is in charge of developing a light weight method to detect any anomalies in the Internet access of end users and in evaluating the importance of these anomalies (how many destinations impacted, the absolute value of the changes over impacted paths). The method in its current version is based on pings sent regularly to a finite set of landmarks and tracked over time. It allows to detect any shifts in the delays that look abnormal and to estimate the number of Internet destinations that would experience the same problem. By deduction, this allows to estimate the importance of the event and to get information on its location with respect to the probing machine. The tool is described in [15] and will be the subject of integration within the Grenouille client and experiments in real network conditions.

8.3. European Initiatives

OneLab 1 & 2 (2006-2010) :

OneLab has been financed by grants from the European Framework Programmes FP6 and FP7. We refer to each successive round of funding as a different phase of the project. To date there are two phases:

OneLab1 This phase of the project ran from September 2006 to August 2008. The central aim was to establish an autonomous European testbed for research on the future Internet, which was achieved through the creation of the PlanetLab Europe testbed. Additional aims were to extend, deepen, and federate this testbed: extension to new technologies, notably wireless; deepening through adding monitoring capabilities; and federating with the global PlanetLab system.

OneLab2 This second and more extensive phase (running for 27 months from September 2008 to November 2010) aims to build on the foundations laid under OneLab1, and continue the project of extension, deepening, and federating. Extension now includes "customer" testbeds including SAC testbeds, wireless testbeds, and content-based testbeds. Deepening continues with the incorporation of some major European measurement infrastructures: DIMES and ETOMIC. Federation continues with federation between PlanetLabs, extending to PlanetLab Japan, as well as federation with the "customer" testbeds, such as the Haggle and ANA testbeds.

IST STREP WSN4CIP (2009-2011):

PLANETE is part of the IST WSN4CIP project. Its goal is to provide solutions that use WSN to protect Critical Infrastructures.

FP7 STREP ECODE (2008-2011) (URL http://www.ecode-project.eu/):

ECODE is an FP7 STREP project that involves in addition to the Planète group, several European partners as Alcatel Belgium, Univ. Liège, Univ. of Louvain, LAAS and Univ. of Lancaster. The project started in September 2008 and will last until September 2011. ECODE stands for Experimental COgnitive Distributed Engine. The goal of the 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.

Within this project, the Planète group is responsible of the adaptive sampling and management use case. Our goal is to develop an autonomous system for network monitoring and traffic management. Starting from a set of measurement tasks like for example the calculation of the traffic matrix, the estimation of flow sizes and rates, the prediction of flow rate increase/decrease, or the detection of anomalies, the system will configure the sampling rates in network routers so as to optimize the accuracy while limiting the overhead (volume of collected traffic, packet processing and memory access in routers). The system will include modules to sample the network, collect the sampled data, analyze it, find the optimal sampling rates, and configure routers accordingly.

8.4. International Activities

Ubisec (2004-2010): is an associated team between UC Irvine (Prof. G.Tsudik) and INRIA Planète project-team.

The objectives of the UbiSec associated team is to understand and tackle problems related to infrastructure-less security, nano-security and anonymous association/routing. The team was prolongated for 3 years in November 2007.

- COMMUNITY Associated team (2009-2010): PLANETE is associated 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 http://inrg.cse.ucsc.edu/community/.
- Roseate (STIC AmSud): This project (2008-2012) 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. The collaboration was prolongated for two years in November 2010.
- STIC Tunisia: (2007-2010) Collaboration with Sonia Gammar from Professor Farouk Kamoun's team at ENSI (Tunis) in the context of a STIC Tunisia project on Security and Monitoring of Hybrid Wireless Mesh Networks. In this project, we co-supervise a PhD student from University of Tunis (Amine Elabidi) working on Data oriented Networking Architecture.

9. Dissemination

9.1. Animation of the scientific community

Walid Dabbous served in the programme committees of Mobiquitous 2010, ICC'10 CISS (Communication and Information System Security Symposium), GC'09 CISS, and was co-chair of the ROADS'09 workshop co-located with SOSP. 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 and head of the scientific committee of the UbiNet Master program launched in 2009 at University of Nice Sophia Antipolis (see http://ubinet.inria.fr). He also served as an expert to the European Commission to evaluate EC funded projects.

Claude Castelluccia served in the program committees of the following international conferences: Wisec2010, SESOC2010, WWW2010, ACM WiSEC2009, IEEE SECON2009 and SARSII2009. He is the co-founder of the ACM WiSec (Wireless Security) conference. He is the editor of the area "Protocols for Mobility" of the ACM SIGMOBILE Mobile Computing and Communications Review (MC2R).

Thierry Turletti Senior ACM and IEEE member, served in 2010 in the program committees of the following international conferences: Packet Video10, the 3rd International Workshop on mobile Video Delivery (Movid)'10 and the 1st International Conference on Wireless and Ubiquitous Systems (ICWUS)10. Since 2001, he is associated editor of the Wireless Communications, Mobile Computing (WCMC) Weslay Journal published by John Wiley & Sons. He is also part of the Editorial Board 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 area editor for ACM Computer Communication Review from 2005 to 2010. He served (is serving) on the Technical Program Committee for several conferences as Infocom 2004, 2005, 2009, 2010 and 2011, ACM IMC 2005 and 2010, PAM 2004 and 2005, ICNP 2002 and 2005, Comsnets 2010, Algotel 2009, ITC 2009, Broadnets 2008, WNS2 2007 and 2008, WinMee 2008, PFLDnet 2008, SECON 2007, etc. He is currently member of the CUMIR committee at INRIA Sophia-Antipolis (Commission des Utilisateurs des Moyens Informatiques).

Vincent Roca is strongly involved in the RMT and MSEC working groups at the IETF. He was part of the Program Committee of RHDM'02, ING'03, ING'04, ING'05. He also serves as an expert in RNRT commission on network protocols and architecture in 2004, 2005 and 2006. Arnaud Legout was PC co-chair of the ICCCN 2009 conference track on P2P networking. He was member of the scientific committee for the summer school RESCOM'2008, he has served as a PC member of CoNext'2008, SIGCOMM'2007 (PC heavy). 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 is reviewer for Computer Communications, IEEE Letters of communications and SIGCOMM CCR. He gave an interview on Privacy and owner's Data control for the SVM magazine August 2009. In 2010, he served in the program committees of the following international conferences: IWTMP2PS 2010, WiMoN 2010, WesT 2010, ACC 2010. He is member of the editorial board of the International Journal of peer-to-peer networks (IJP2P). He also reviewed articles for TPDS (IEEE Transactions on Parallel and Distributed Systems), SIGCOMM CCR (Computer Communication Review), Computer Communications, IEEE letters of communications and Computer Networks.

9.2. PhD Theses and Internships

9.2.1. PhD defended in 2010

1. Mohamed Karim Sbai defended his PhD titled "Architecture for content sharing in wireless networks" on October 1st at INRIA Sophia Antipolis. The research work was supervised by Walid Dabbous and Chadi Barakat.
2. Mathieu Lacage defended his PhD titled "Experimentation Tools for Networking Research" on November 15th at INRIA Sophia Antipolis. His research work was supervised by Walid Dabbous.
3. Amine Ismail defended his PhD titled "Optimisation of IP protocols and applications over broadcast links" on June 28th. His research work was co-supervised by Walid Dabbous and Antoine Clerget from UDcast.
4. Mathieu Cunche defended his PhD titled "Codes AL-FEC hautes performances pour las canaux à effacements: variations autour des codes LDPC" on May 10th at INRIA Grenoble. His thesis was supervised by Vincent Roca.

9.2.2. Ongoing PhDs

1. Sana Ben Hamida works on “Embedded System Security”.
2. Mohamad Jaber works on “Detection and Troubleshooting of Internet Anomalies”.
3. Imed Lassoued works on “Adaptive Monitoring and Management of Internet Traffic”.
4. Stevens Le Blond works on “Next Generation Peer-to-Peer Infrastructures”.
5. Pere Manils works on “Security of the TOR network”.
6. Daniele Perito works on “Critical Infrastructure Protection”.
7. Rao Naveed Bin Rais works on “Adaptive Communication Mechanisms for Networks with Episodic Connectivity”.
8. Ludovic Jacquin works on “High Bandwidth Secure Communications”.
9. Shafqat Ur-Rehman works on “Benchmarking Methodology for Network Protocols Evaluation”.
10. Ashwin Satish Rao works on “Performance evaluation of communication networks”.
11. Amir Krifa works on “File sharing in wireless ad hoc networks”.
12. Abdelberi Chaabane works on “Secure localizations in Wireless Sensor networks”.
13. Ferdaouss Mattoussi works on “Optimizing FEC strategies for wireless communications”.

9.2.3. Training activities

1. Chérifa Boucetta,
   Duration of the stay: 4 months from Feb 15th to June 15th 2010
   Topic: Security of localization protocols in Wireless Sensor Networks
   Prepared degree: Master Thesis in Computer Science.
   Affiliation: ENSI, University of Manouba, Tunisia.
2. Abdeleberi Chaabane,
   Duration of the stay: 6 months from October 9th 2009 to March 31st 2010
   Topic: Large Scale Overlays Monitoring
   Prepared degree: Master Thesis in Computer Science.
   Affiliation: ENSI, University of Manouba, Tunisia.
3. Mariem Abdelmoula,
   Duration of the stay: 6 months from March 1st to August 31st 2010
   Topic: New communication architecture for data delivery in heterogeneous networks prone to disruptions in connectivity
   Prepared degree: IFI-Ubinet Master
   Affiliation: University of Nice Sophia Antipolis
4. Matin Hernan Ferrari,
   Duration of the stay: 6 months from Apris 1st to September 30th 2010
   Topic: NEPI, an experiment plane for experimentation testbeds
   Prepared degree: IFI-Ubinet Master
   Affiliation: University of Nice Sophia Antipolis
5. Kamel Trimeche,
   Duration of the stay: 4 months from February 8th to June 8th 2010
   Topic: Implementation of a multimedia evaluation toolkit for the ns-3 simulator
   Prepared degree: Engineering diploma.
   Affiliation: ENSI, Tunisia.

6. Nabil Echaouch,
   Duration of the stay: 7.5 months from February 2nd to June 2nd then since September 15th 2010.
   Topic: New communication architecture for data delivery in heterogeneous networks prone to disruptions in connectivity
   Prepared degree: Master
   Affiliation: ENSI, Tunisia.
7. Carlo D'Elia,
   Duration of the stay: 4 months from March 8th to July 8th 2010.
   Topic: Analysis of wireless experimentations
   Prepared degree: PhD
   Affiliation: Politecnico di Bari, Italy.
8. Ilias Chatzidrosos,
   Duration of the stay: 3.5 months from April 15th to July 31st 2010.
   Topic: Experimental evaluation of P2P streaming
   Prepared degree: PhD
   Affiliation: KTH, Sweden.
9. Saghar Estehghari,
   Duration of the stay: 12 months since January 2010.
   Topic: Owner-Centric Networks.
   Prepared degree: MSc Information Security
   Affiliation: UCL, London.
10. Kazuhisa Matsuzono,
   Duration of the stay: 1.5 months from February 1st to March 15th 2010
   Topic: Implementation of the FECFRAME framework.
   Prepared degree: PhD
   Affiliation: Keio University, Japan.

9.3. Teaching

Networks and protocols: Undergraduate course at Ecole Polytechnique, Palaiseau, by W. Dabbous (36h).

Evolving Internet: architectural challenges Course at the IFI-UbiNet Master program, University of Nice-Sophia Antipolis, by W. Dabbous and C. Barakat (42h).

An introduction to Internet monitoring: Course at *(i)* Telecom Paris, 2009-2010, and *(ii)* ETH Zurich, 2009, C. Barakat (3h).

Wireless networking: Course at Master RTM, IUP Avignon, 2009 - 2010, C. Barakat (7h).

Local Aarea Networks: Course at IUT of the University of Nice-Sophia Antipolis, 2007-2010, C. Barakat (21h+ 10.5h practical work).

Introduction to Networking: Course at IUT Nice, Licence LPSIL, 2006-2008, C. Barakat (15h).

Voice over IP: Course at *(i)* Master TIM, UNSA, 2007 - present, *(ii)* Master RTM, IUP Avignon, 2008, C. Barakat (7h).

Network Simulator ns-2: Course at Master RTM of IUP Avignon, 2008, C. Barakat (7h).

Peer-to-peer networks: Course in the UbiNet master at University of Nice-Sophia Antipolis 2010 (21h), by Arnaud Legout

Peer-to-peer networks: Course in the IUP GMI Avignon 2010 (24h + 21h practical work), by Arnaud Legout.

Wireless Security: Course given to the students of the Ensimag "crypto and security" Master 2, Ensimag, Grenoble by C. Castelluccia (20h).

Wireless Security: Course given to the students of the Ensimag/INPG “MOSIG” Master 2, Ensimag/INPG, Grenoble by C. Castelluccia (12h).

Wireless Communications: Undergraduate course at Polytech’ Grenoble, on Wireless Communications, by V. Roca (12h).

Networking: Undergraduate course at IUT-2’ (UPMF University), on network Communications, by V. Roca (24h).

Networks and Telecommunications: Programming and Networking Courses given to the students of ENSIMAG, Grenoble by Mohamed Ali Kaafar (40h).

Computer Networks: Programming Courses given to the students of Phelma/INPG, Grenoble by Mohamed Ali Kaafar (12h).

Internet Privacy: Different Seminars given to master-level students in 2010.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] M. Cunche. *Codes AL-FEC hautes performances pour las canaux à effacements: variations autour des codes LDPC*, Joseph Fourier University, Grenoble, May 2010.

[2] M. A. Ismail. *Study and Optimization of Data Protection, Bandwidth Usage and Simulation Tools for Wireless Networks*, University of Nice-Sophia Antipolis, June 2010.

[3] M. Lacage. *Outils d’Expérimentation pour la Recherche en Réseaux*, University of Nice-Sophia Antipolis, November 2010.

[4] M. K. Sbai. *Architecture for Content Sharing in Wireless Networks*, University of Nice-Sophia Antipolis, October 2010.

Articles in International Peer-Reviewed Journal

[5] M. Borhan Uddin, C. Castelluccia. *Toward Clock Skew Based Services in Wireless Sensor Networks*, in "International Journal of Sensor Networks (IJSNet)", 2010.

[6] D. Dujovne, T. Turletti, F. Filali. *A Taxonomy of IEEE 802.11 Wireless Parameters and Open Source Measurement Tools*, in "IEEE Surveys and Tutorials", Second Quarter 2010, vol. 12, n^o 2, p. 249-262.

[7] M. Lacage, M. Ferrari, M. Hansen, T. Turletti, W. Dabbous. *NEPI: Using Independent Simulators, Emulators, and Testbeds for Easy Experimentation*, in "ACM Operating Systems Review (OSR)", January 2010, vol. 43, n^o 4.

[8] S. Le Blond, A. Legout, W. Dabbous. *Pushing BitTorrent Locality to the Limit*, in "Computer Networks", 2010, vol. doi:10.1016/j.comnet.2010.09.014.

[9] T. Spyropoulos, R. N. Bin Rais, T. Turletti, K. Obraczka, A. Vasilakos. *Routing for disruption tolerant networks: taxonomy and design*, in "Wirel. Netw.", November 2010, vol. 16, p. 2349–2370, http://dx.doi.org/10.1007/s11276-010-0276-9.

Articles in Non Peer-Reviewed Journal

[10] C. CASTELLUCCIA. *Internet et vie privée, des frères ennemis ?*, in "Pour La Science", janvier 2010, n^{o} 66.

[11] W. DABBOUS. *L'architecture d'Internet à l'ère du mouvement*, in "Pour La Science", janvier 2010, n^{o} 66.

International Peer-Reviewed Conference/Proceedings

[12] S. BEN HAMIDA, J. B. PIERROT, C. CASTELLUCCIA. *Empirical Analysis of UWB Channel Characteristics for Secret Key Generation in Indoor Environments*, in "proceedings of The 21st IEEE International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC'10", Istambul, Trukey, September 2010.

[13] 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.

[14] C. BOUCETTA, M. A. KAAFAR, M. MINIER. *How Secure are Secure Localizations protocols in WSNs*, in "The ICST Conference on Wireless Sensor Network (WSN) Systems and Software", Miami, ICST, December 2010.

[15] R. CASCELLA, C. BARAKAT. *Estimating the access link quality by active measurements*, in "proceedings of the 22nd International Teletraffic Congress (ITC 22)", Amsterdam, Netherlands, September 2010.

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

[17] C. CASTELLUCCIA, K. ELDEFRAWY, G. TSUDIK. *Link-Layer Encryption Effect on the Capacity of Network Coding in Wireless Networks*, in "proceedings of IEEE Infocom MiniConference", San Diego, CA, March 2010.

[18] A. CHAABANE, P. MANILS, M. A. KAAFAR. *Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network*, in "IEEE International Conference in Network and System Security (NSS)", Melbourne, IEEE, September 2010.

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

[20] L. A. GRIECO, C. BARAKAT. *A Frequency Domain Model to Predict the Estimation Accuracy of Packet Sampling*, in "proceedings of the IEEE Infocom MiniConference", San Diego (CA), March 2010.

[21] M. A. ISMAIL, G. PIRO, L. A. GRIECO, T. TURLETTI. *An Improved IEEE 802.16 WiMAX Module for the NS-3 Simulator; Best Student Award Paper*, in "proceedings of ICST Simutools'2010", Torremolinos, Malaga, Spain, March 2010.

[22] M. JABER, C.-C. NGO, C. BARAKAT. *A view from inside a distributed Internet coordinate system*, in "proceedings of the Global Internet Symposium at IEEE Infocom", San Diego (CA), March 2010.

[23] L. JACQUIN, V. ROCA, J.-L. ROCH, M. AL ALI. *Parallel arithmetic encryption for high-bandwidth communications on multicore/GPGPU platforms*, in "ACM workshop on Parallel Symbolic Computation (PASCO 2010)", July 2010.

[24] M. A. KAAFAR, P. MANILS. *Why Spammers should thank Google*, in "ACM EUROSYS on Social Network Systems (SNS 2010)", Paris, ACM, April 2010.

[25] A. KRIFA, I. LASSOUED, C. BARAKAT. *Emulation Platform for Network Wide Traffic Sampling and Monitoring*, in "proceedings of the 1st International Workshop on TRaffic Analysis and Classification (TRAC)", Caen, France, June 2010.

[26] I. LASSOUED, C. BARAKAT. *Adaptive Multi-task Monitoring System Based on Overhead Prediction*, in "proceedings of the ACM CoNext PRESTO workshop on Programmable Routers for Extensible Services of Tomorrow", Philadelphia (PA), November 2010.

[27] S. LE BLOND, A. LEGOUT, F. LEFESSANT, W. DABBOUS, M. A. KAAFAR. *Spying the World from your Laptop - Identifying and Profiling Content Providers and Big Downloaders in BitTorrent*, in "proceedings of LEET'10", San Jose, CA, USA, April 2010.

[28] K. MATSUZONO, J. DETCHART, M. CUNCHE, V. ROCA, H. ASAEDA. *Performance Analysis of a High-Performance Real-Time Application with Several AL-FEC Schemes*, in "35th IEEE Conference on Local Computer Network (LCN'10)", Denver, Colorado, U.S.A., October 2010.

[29] A. S. RAO, A. LEGOUT, W. DABBOUS. *Can Realistic BitTorrent Experiments Be Performed on Clusters?*, in "proceedings of P2P'2010", Delft, Netherlands, August 2010.

[30] M. K. SBAI, E. SALHI, C. BARAKAT. *P2P content sharing in spontaneous multi-hop wireless networks*, in "proceedings of the second International Conference on COMmunication Systems and NETworkS (COMSNETS)", Bengalore, India, January 2010.

Workshops without Proceedings

[31] S. LE BLOND, P. MANILS, A. CHAABANE, M. A. KAAFAR, A. LEGOUT, C. CASTELLUCCIA, W. DABBOUS. *De-anonymizing BitTorrent Users on Tor*, in "poster session at the 7th USENIX Symposium on Network Design and Implementation (NSDI '10)", San Jose, CA, USA, April 2010.

[32] P. MANILS, A. CHAABANE, S. LE BLOND, M. A. KAAFAR, A. LEGOUT, C. CASTELLUCCIA, W. DABBOUS. *Compromising Tor Anonymity Exploiting P2P Information Leakage*, in "ACM Hot Topics in Privacy Enhancing Technologies", Berlin, ACM, July 2010.

[33] A. S. RAO, A. LEGOUT, W. DABBOUS. *BitTorrent Experiments on Testbeds: A Study of the Impact of Network Latencies*, in "JDIR'10", Sophia Antipolis, France, March 2010.

Scientific Books (or Scientific Book chapters)

[34] T. SPYROPOULOS, R. N. BIN RAIS, T. TURLETTI, K. OBRACZKA, A. VASILAKOS. *3*, in "DTN Routing: Taxonomy & Design", CRC Press, 2010.

Research Reports

[35] B. Adamson, V. Roca, H. Asaeda. *Security and Reliable Multicast Transport Protocols: Discussions and Guidelines*, May 2010, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-sec-discussion-05.txt>.

[36] R. N. Bin Rais, T. Turletti, K. Obraczka. *MeDeHa - Efficient Message Delivery in Heterogeneous Networks with Intermittent Connectivity*, March 2010, http://hal.inria.fr/inria-00464085_v1/.

[37] S. Galanos, O. Peck, V. Roca. *RTP Payload Format for Reed Solomon FEC*, August 2010, IETF FECFRAME Working Group, Work in Progress: <draft-galanos-fecframe-rtp-reedsolomon-02>.

[38] S. Galanos, O. Peck, V. Roca. *RTP Payload Format for Reed Solomon FEC*, March 2010, IETF FECFRAME Working Group, Work in Progress: <draft-galanos-fecframe-rtp-reedsolomon-01>.

[39] S. Le Blond, A. Legout, F. Lefessant, W. Dabbous. *Angling for Big Fish in BitTorrent*, January 2010.

[40] P. Manils, A. Chaabane, S. Le Blond, M. A. Kaafar, A. Legout, C. Castelluccia, W. Dabbous. *Compromising Tor Anonymity Exploiting P2P Information Leakage*, April 2010.

[41] T. Paila, R. Walsh, M. Luby, V. Roca, R. Lehtonen. *FLUTE - File Delivery over Unidirectional Transport (revised)*, January 2010, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-09.txt>.

[42] T. Paila, R. Walsh, M. Luby, V. Roca, R. Lehtonen. *FLUTE - File Delivery over Unidirectional Transport (revised)*, January 2010, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-10.txt>.

[43] T. Paila, R. Walsh, M. Luby, V. Roca, R. Lehtonen. *FLUTE - File Delivery over Unidirectional Transport (revised)*, March 2010, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-11.txt>.

[44] V. Roca, B. Adamson. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, July 2010, IETF RMT Working Group (individual document), Work in Progress: <draft-ietf-rmt-newfcast-01.txt>.

[45] V. Roca, B. Adamson. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, October 2010, IETF RMT Working Group (individual document), Work in Progress: <draft-ietf-rmt-newfcast-02.txt>.

[46] V. Roca, M. Cunche, J. Lacan, A. Bouabdallah, K. Matsuzono. *Reed-Solomon Forward Error Correction (FEC) Schemes for FECFRAME*, March 2010, IETF FECFRAME Working Group, Work in Progress: <draft-roca-fecframe-rs-02.txt>.

[47] V. Roca, M. Cunche, J. Lacan, A. Bouabdallah, K. Matsuzono. *Simple Reed-Solomon Forward Error Correction (FEC) Schemes for FECFRAME*, October 2010, IETF FECFRAME Working Group, Work in Progress: <draft-roca-fecframe-simple-rs-00.txt>.

[48] V. Roca, M. Cunche, J. Lacan, A. Bouabdallah, K. Matsuzono. *Simple Reed-Solomon Forward Error Correction (FEC) Schemes for FECFRAME*, July 2010, IETF FECFRAME Working Group, Work in Progress: <draft-roca-fecframe-rs-03.txt>.

[49] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Simple Reed-Solomon Forward Error Correction (FEC) Schemes for FECFRAME*, October 2010, IETF FECFRAME Working Group, Work in Progress: <draft-roca-fecframe-simple-rs-01.txt>.

[50] V. ROCA, M. CUNCHE, J. LACAN. *LDPC-Staircase Forward Error Correction (FEC) Schemes for FECFRAME*, October 2010, IETF FECFRAME Working Group, Work in Progress: <draft-roca-fecframe-ldpc-01.txt>.

[51] V. ROCA, A. FRANCILLON, S. FAURITE. *TESLA source authentication in the ALC and NORM protocols*, April 2010, IETF Request for Comments, RFC 5776 (Experimental).

[52] V. ROCA. *Simple Authentication Schemes for the ALC and NORM Protocols*, July 2010, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-simple-auth-for-alc-norm-03.txt>.

[53] S. UR-REHMAN, T. TURLETTI, W. DABBOUS. *"Benchmarking of Wireless Experimentations"*, October 2010.

Other Publications

[54] R. N. BIN RAIS, M. MENDONCA, T. TURLETTI, K. OBRACZKA. *"Message Delivery in Heterogeneous Disruption-prone Networks"*, September 2010, Invited demo presentation at The ACM second Wireless of the Students, by the Students, for the Students (S3).

[55] R. N. BIN RAIS, M. MENDONCA, T. TURLETTI, K. OBRACZKA. *"Message Delivery in Heterogeneous Disruption-prone Networks"*, September 2010, Demo description in Proc. of ACM Mobicom.

[56] J. LACAN, E. LOCHIN, P.-U. TOURNOUX, A. BOUABDALLAH, V. ROCA. *On-the-fly coding for time-constrained applications*, September 2010, http://arxiv.org/pdf/0904.4202v3.

[57] J. LACAN, E. LOCHIN, P.-U. TOURNOUX, A. BOUABDALLAH, V. ROCA. *On-the-fly coding for time-constrained applications*, February 2010, http://arxiv.org/pdf/0904.4202v2.