INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team PLANETE

Protocoles et Applications pour l'Internet

Sophia Antipolis - Méditerranée, Grenoble - Rhône-Alpes

Theme : Networks and Telecommunications

Table of contents

1. Team

Research Scientist

Walid Dabbous [Team Leader, Research Director, Inria, HdR]
Claude Castelluccia [Research Director, Inria, HdR]
Thierry Turletti [Research Scientist, Inria, HdR]
Chadi Barakat [Research Scientist, Inria, HdR]
Mohamed Ali Kaafar [Research Scientist, Inria]
Arnaud Legout [Research Scientist, Inria]
Vincent Roca [Research Scientist, Inria]

Technical Staff

Bilel Ben Romdhanne [Associate Engineer]
Alina Quereilhac [Associate Engineer, since December 2009]
Lionel Giraud [Associate Engineer until January 2009]
Jonathan Detchart [Associate Engineer ADT since October 2009]
Mads Hansen [Associate Engineer ADT until August 2009]
Amir Krifa [Expert Engineer]
Mathieu Lacage [Dream Engineer]
Faker Moatamri [Expert Engineer since April 2009]
Thierry Parmentelat [Dream Engineer]
Anil Kumar Vengalil [Expert Engineer]
Baris Metin [Expert Engineer]

PhD Student

Sana Ben Hamida [Funding CEA LETI]
Mathieu Cunche [Funding ANR contract]
Diego Dujovne [Funding Argentinian Scholarship, until May 2009]
Aurélien Francillon [Funding Ubisec&Sens project until October 2009]
Amine Ismail [Funding CIFRE Scholarship with UDcast]
Mohamad Jaber [Funding MESR Scholarship]
Ludovic Jacquin [Minalogic Inria grant since October 2009]
Mathieu Lacage [Inria Dream Engineer]
Imed Lassoued [Funding ECODE project]
Stevens Le Blond [Funding Inria CORDIS Scholarship]
Pere Manils [Finding Inria CORDIS, since September 2009]
Daniele Perito [Funding WSN4CIP IST project]
Naveed Bin Rais [Funding Pakistanian Scholarship]
Mohamed Karim Sbai [Funding ITEA ExpeShare project]
Ashwin Satish Rao [Funding OneLab2 project since September 2009]
Mate Soos [Funding Inria grant until September 2009]
Shafqat Ur Rehman [Funding OneLab2 project]

Post-Doctoral Fellow

Roberto Cascella [Funding ECODE project since January 2009]
Mate Soos [Funding Inria grant since October 2009]

Visiting Scientist

Emiliano DeCristofano [Visiting PhD, from September to December 2009]
Giovanni Di Stasi [Visiting PhD, from March 2009 to April 2009]
Luigi Alfredo Grieco [Invited Professor, from March 2009 to June 2009]
Giuseppe Piro [Visiting PhD, June 2009 and November 2009]
Claudio Soriente [Visiting PhD, until January 2009]

Administrative Assistant

Dominique Guédon [Sophia]
Helen Pouchot [Grenoble]

Other

Mariem Abdelmoula [from February 2009 to June 2009]
Alice Albano [from February 2009 to July 2009]
Maher Ben Yahmed [from February 2009 to June 2009]
Aldelberi Chaabane [from February 2009 to December 2009]
Ludovic Fardel [from February 2009 to August 2009]
Martin Ferrari [from May 2009 to September 2009]
Gaël Grimaud [from April to June 2009]
Adrien Gallais [from June 2009 to July 2009]
Cao Cuong Gno [from March 2009 to August 2009]
Pere Manils [from April 2009 to August 2009]
Guillaume Séguin [from June 2009 to August 2009]
Emna Salhi [until February 2009]
Teresa Siso Nadal [from April 2009 to September 2009]
Marcel Sutter [until April 2009]

2. Overall Objectives

2.1. Overall Objectives

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.

3. Scientific Foundations

3.1. Scientific foundations

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

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

In order to carry out our approach as well as possible, it is important to attend and contribute the 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 research 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 contribut to the future internet architecture.

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 the ever be larger that 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 the today 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 specifying explicitly its location, the network will transparently return with closest instance of the content. You can also request a specific service to 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 in 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 due to a number of factors such as node mobility, link instability, power-aware protocols that, for example, turn nodes off periodically, etc., the network will not be connected all the time. 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 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 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 that these broadcasting systems be seamlessly integrated to the Internet, so that users be able to 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 network 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 support 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

The Internet was not designed to operate in an completely open and hostile environment. It was designed by researchers that trust each other and security 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 intrusions 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 on security in wireless, ad hoc and sensor networks, mainly the design of new key exchange protocols and of secured routing protocols. We work also on location privacy techniques and 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 about the architecture of the Internet with security as a major design requirement, instead of an after-thought.

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.

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.

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 the work on extensions for what we have already proposed, 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 or 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.

Network Evaluation Platforms

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 deploying 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 increase 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 envi-

ronment 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 Simulator

ns-3 is the followup to the wildly successful ns-2 project. ns-2 was, for many years, the reference network simulator for IP networks to the point that more than 50% or all papers published in many conferences and journals used ns-2 to validate their research. Despite (or because of) this success, ns-2 is showing its age: its architecture suffers from a number of important problems which could not be solved with a thorough redesign. This lead a number of US-based researchers to start the development of ns-3 from scratch with NSF funding. Through our involvement in the ns-3 project from its very early stages (we were invited to its kickoff meeting), we contributed to the architecture and the implementation of its core facilities. Most notably, we implemented the event scheduler, the packet data structure, the tracing subsystem, important aspects of the object model, and the default network node programming interface. We also worked on the first version of the UDP/IPv4 stack. This work was based on YANS ("Yet Another Network Simulator") which we developed just prior to starting work on ns-3. See http://www.nsnam.org for more details.

5.2. NEPI

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 attempts to define a common API to perform all the above-mentioned tasks and allows users to access these features through a simple yet powerful graphical user interface.

5.3. OneLab build of PlanetLab

In the context of the OneLab project, our project-team is in charge of the codebase management for the PlanetLab Europe platform. This codebase was initially created from an import of the standard PlanetLab software, on top of which we have implemented a variety of improvements. 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 any user a consolidated view of all federating resources regardless of the user's affiliation. We have also contributed various improvement to handle more heterogeneous types of hardware, like e.g. wireless or multi-homed connectivity. Until 2007, the collaboration scheme with Princeton University has been upstream-downstream: we were free to make any change to the Princeton code provided that we adhered some standard interfaces, and Princeton was free to import any of our changes if they seemed interesting. We have moved in 2008 towards a co-development model, where we would share the same codebase as Princeton, so as to ease cross-importations that, over time, have become more and more frequent, but time-consuming. 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. Seehttp://planet-lab.eu for more details.

Last year, we have kept on developping new features and enhancements for the PlanetLab software. A substantial part of our activities have been devoted to bringing the project to a more mature stage. In a first direction, we have now completed the move towards an almost full co-development model; all the OneLab-specific features have now been merged into the mainstream codebase that is located under http://svn.planet-lab.org/; the builds that are published for PlanetLab Europe, and for the general public, can and that can be found under http://build.onelab.eu/, now differ from the stock PlanetLab distribution only by a few tweaks. Secondly, we have contributed a validation framework that allows continuous integration, as daily builds now run a set of non-regression tests. Last, we have brought more general support for the underlying Linux distribution, that allows to build the software for different release levels of Fedora and CentOS. Leveraging on these contributions, we've ben ale to take an active part in the delivery of version 4.2 earlier this year, that brought man innovations to the core system, including a complete rewrite of the network isolation mechanisms (known as vnet), as well as a new module for punching holes in the slice-isolation layer (known as vsys). We are now involved in the making of version 5.0, that aims at defining a more extensible data model for handling much more heterogeneous resources.

This year, we started with releasing the latest stable version of Planetlab software, MyPLC 4.3, and deployed this on PLE. We did 15 subsequent minor release for MyPLC since then, where each had many bug fixes as well as new features. Dealing with SSL certificate issues we setup another server for Planetlab Europe running as the boot server (boot.planet-lab.eu). We have also worked together with Princeton to release and deploy MyOps, a monitoring system for MyPLC which also helps with automated operational tasks. We again collaborated with PLC to coordinate works in SFA and sfatables (access and admission control tool for SFA) as well as the initial work for SFA user interface.

5.4. WSN Security Protocols

We have developped the following TinyOS modules:

- **TinyRNG:** TinyRNG is a random number generator of a cryptographic quality. It uses entropy collection and accumulates entropy into two pools, that makes possible to provide forward and backward security. One of the source of entropy comes from the erroneous packet received from the radio, with careful selection between what's could be modified by an attacker and what could not be attacker controlled. TinyRNG provide standard TinyOS Random interface and it is expected to be extremely easy to integrate into existing projects.
- **RoK module**: RoK is a novel key exchange protocol for wireless sensor networks.
- **CDA**: CDA is a module that provide encryption of convergecast traffic.

5.5. MultiCast Library Version 3

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

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. Prototype 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, via http://planete.inria.fr/software/WisMon/.

Wextool

Wextool aims to set up, run and make easier the analysis of wireless experiments. It is a flexible and scalable open-source tool that covers all the experimentation steps, from the definition of the experiment scenario to the generation and storage of results. Sources and binaries of Wextool 1.0 are available under the GPLv2 licence at http://planete.inria.fr/Software/Wextool/.

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 packets 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.

BitHoc

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 at http://planete.inria.fr/bithoc. 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.

TICP

TICP [45]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. More details on the protocol and the validation results can be found at http://planete.inria.fr/ticp/ and in the following publications [36], [12].

6. New Results

6.1. Data Centric Networking

Participants: Chadi Barakat, Mathieu Cunche, Walid Dabbous, Diego Dujovne, Aurélien Francillon, Amine Ismail, Mohamed Ali Kaafar, Mathieu Lacage, Naveed Bin Rais, Vincent Roca, Emna Salhi, Karim Sbai, Thierry Turletti.

The work on data centric architectures is a follow-up and federation of three of our previous activities (adaptive multimedia transmission protocols for heterogeneous networks, data dissemination paradigms and peer-to-peer systems). We present hereafter the results obtained in 2009 in this area.

- **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 [52] ("proposed standard" maturity level). We also performed a detailed performance comparison of LDPC-Staircase, Reed-Solomon and Raptor codes in [23]. We also studied the possibility of light-weight software decoding of Reed-Solomon codes in [16].

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 [39].

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 [22].

- **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 and LDPC-Staircase codes within the FECFRAME framework [62], [61], [63]. In parallel we have started an implementation of the FECFRAME framework in order to gain an in-depth understanding of the system.

  In the context of robust streaming systems, we also contributed to the analysis of the Tetrys approach, in [51].

- **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). It has recently been accepted as a Working Group Item and WG Last Call should quickly begin [58], [59], [60].

- **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, 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. The document has

been reviewed by IESG, comments addressed, and it is currently in the RFC Editor queue, which means it should soon be published as an RFC [64], [65], [66].

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 [67]. 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. The ideas has been published in [40].

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

  DVB-SH is a new broadcasting standard offering a mobile TV service for handheld devices using hybrid satellite/terrestrial-repeaters solution. A new link layer protection algorithm called Multi-Burst Sliding Encoding (MBSE) has been recently adopted to cope with the long fading time introduced by the direct satellite link. We proposed 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 equipements and have validated the optimization method using intensive experiments with typical usage scenarios under a hardware-emulated wireless link [27].

- **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. We have addressed the problem of routing in intermittently connected wireless networks comprising multiple classes of nodes. We have shown in [13] that proposed solutions, which perform well in homogeneous scenarios, are not as competent in this setting. To this end, we proposed a class of routing schemes that can identify the nodes of highest utility for routing, improving the delay and delivery ratio by 4-5 times. Additionally, we proposed an analytical framework based on fluid models that can be used to analyze the performance of various opportunistic routing strategies, in heterogeneous settings.

  In this research area, another work focuses on efficient message delivery mechanism to enable distribution/dissemination of messages in an internet connecting heterogeneous networks and prone to disruptions in connectivity. We called our protocol MeDeHa for Message Delivery in Heterogeneous, Disruption prone Networks. MeDeHa stores data at the link layer addressing heterogeneity 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) to improve message delivery. Another important feature of MeDeHa is that there is no need to deploy special-purpose nodes such as message ferries, data mules, or throwboxes in order to relay data to intended destinations,

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 existing storage as well as quality-of-service issues such as delivery delay bounds imposed by the application. We have evaluated MeDeHa via simulations using indoor scenarios (e.g. convention centers, exposition halls, museums etc.) and have shown significant improvement in delivery ratio in the face of episodic connectivity.

Then, we have extended the MeDeHa framework to include ad hoc network support, as the earlier version of the framework implementation only had infrastructure mode working. This is the first step towards achieving network heterogeneity. Currently, the implementation is able of supporting wired, infrastructure wireless, and ad hoc networks, and it is implemented within the new Network Simulator 3 (ns-3), which allows simulations as well as emulations. Thus, this implementation will be helpful not only in analyzing different scenarios in the simulator, but also to test the framework on real networks in the future.

These works are the result of collaborations with Thrasyvoulos Spyropoulos from ETH Zurich and Katia Obraczka from University of California Santa Cruz (UCSC). It is done in the context of the COMMUNITY Associated Team (http://planete.inria.fr/COMMUNITY/).

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

We have proposed an efficient joint scheduling and drop policy that can optimize different performance metrics, such as the average delivery rate and the average delivery delay. First, we present 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, in practice. At the end, we are able to associate to each message inside the network a utility message that can be calculated locally, and that allows to compare it to other messages upon scheduling and buffer congestion. We pursue the research in this area by looking for methods to reduce the overhead of the history-collection plane, and by trying to cast existing standard policies within the framework of our study.

- **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 lot 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.

Last year, we presented a first solution to this problem that we refine in [42], [37]. Unlike uni-metric approaches, our solution considers relevant performance metrics together as throughput, sharing and routing overhead. We define a new neighbor selection strategy that balances sharing and diversification efforts and decides on the optimal neighboring scope of a node. We also consider the diversification incentives problem and evaluates the impact of nodes' mobility on the P2P strategy to be adopted. Through extensive simulations, we prove that our solution achieves both better download time and sharing ratio than uni-metric solutions.

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 http://planete.inria.fr/bithoc. It is intended 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 or might not exist. The proposed BitHoc architecture 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 (see [37] for more details on how to construct this membership management overlay). 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.

- **Efficient Wireless LAN Protocols**

  We have worked on two different areas to increase the performance of wireless LAN protocols. First, we have proposed an efficient aggregation mechanism for the upcoming IEEE 802.11n standard. Second, we have worked on efficient PHY rate selection mechanisms for IEEE 802.11 networks.

  We have proposed the Aggregation with Fragment Retransmission (AFR) mechanism to achieve high efficiency at the MAC layer of IEEE 802.11n [9]. In the AFR scheme, multiple packets are aggregated into and transmitted in a single large frame. If errors occur during the transmission, only the corrupted fragments of the large frame are retransmitted. An analytic model has been developed to evaluate the throughput and delay performance of AFR over noisy channels, and to compare AFR with similar schemes in the literature. Optimal frame and fragment sizes have been calculated using this model. Transmission delays are minimized by using a zero waiting mechanism where frames are transmitted immediately once the MAC wins a transmission opportunity. We prove that this mechanism achieves maximum throughput. As a complement to the theoretical analysis, we investigated by simulations the impact of AFR on the performance of realistic application traffic for diverse scenarios: TCP, VoIP and HDTV traffic. The AFR scheme described was developed as part of the 802.11n working group work. It is the result of a collaboration with Tianji Li, David Malone and Douglas Leith from Hamilton Institute in Ireland, Qiang Ni at University of Brunel, England and Yang Xiao from the Dept. of CS at University of Alabama.

6.2. Security in infrastructure-less and constrained networks

Participants: Claude Castelluccia, Mohamed Ali Kaafar, Aurélien Francillon, Daniele Perito, Mate Soos, Pere Manils, Sana Ben Hamida, Abdelberi Chaabane.

- **Software-based program code attestation in wireless sensor networks**

Embedded systems are employed in several critical environments where correct operation is an important requirement. Malicious nodes in a Wireless Sensor Network (WSN) can be used to disrupt the network operation by deviating from the prescribed protocol or to launch internal attacks. Preventing node compromise is difficult; it is therefore desirable to detect compromised nodes to isolate them from the network. This is performed through *code attestation*, i.e., the base station verifies that each of the nodes is still running the initial application and, hence, has not been compromised. Attestation techniques based on tamper-resistant hardware, while possible are not generally available, nor are foreseen to be cost effective for lightweight WSNs nodes.

Software-based attestation is a promising solution for verifying the trustworthiness of inexpensive, resource constrained sensors, because it does not require dedicated hardware, nor physical access to the device. Previously proposed techniques are based on a challenge-response paradigm. In this paradigm, the verifier (usually the base station) challenges a prover (a target device) to compute a checksum of its memory. The prover either computes the checksum using a fixed integrity verification routine or downloads it from the verifier right before running the protocol. In practice, memory words are read and incrementally loaded to the checksum computation routine. To prevent replay or pre-computation attacks, the verifier challenges the prover with a nonce to be included in the checksum computation. Since the verifier is assumed to know the exact memory contents and hardware configuration of the prover, it can compute the expected response and compare it with the received one. If values match, the node is genuine, otherwise, it has most likely been compromised.

This work highlights shortcomings of several code attestation techniques for embedded devices and shows practical attacks against them. First, we developped a *Rootkit* for embedded systems – a malicious program that allows a permanent and undetectable presence on a system – that circumvents attestation by hiding itself in non-executable memories. The implementation of this attack uses a technique called *Return-Oriented Programming* (ROP), a generalization of return-into-libc. ROP can be used by the adversary to compromise the node and perform arbitrary computations without inje cting code. Node compromise is achieved by reusing and controlling pieces of code already pr esent in the device's memory. Second, we designed an attack that uses code compression to free memory space whi ch can be used to hide malicious code.

We also developped some specific attacks against previously proposed attestation protocols, ultimately showing the difficulty of software-based attestation design.

This work has been published at the ACM CCS'09 [18]

- **Implantable Medical Device Security**

  In order to facilitate communication and data readout, new generations of Implantable Medical Devices (IMDs), such as pacemakers, are equipped with radio transceivers. Such interfaces makes it convenient for medical professionals to get access to the data they need but they also introduce some unique security and privacy challenges, access to personal data and the unauthorized modification of IMD parameters being the most prominent.

  In order to prevent unauthorized access to IMDs, conventional solutions, based on public-key cryptography or on preloaded secret keys cannot be directly applied since they typically also prevent access to IMDs in emergency scenarios where the IMD needs to be accessible to emergency ambulance staff. IMDs therefore create a tension between access control, i.e., patient privacy, and patient safety. Several solutions were proposed to address this problem. Some solutions are based on external devices such as access tokens and communication cloakers, whereas others rely on close-range communication channels (e.g., RFID). In addition to possibly being stolen, lost, or simply forgotten by the patient, external devices also serve as a constant reminder to the patient of her/his condition. Access control solutions based on close-range communication have the advantage of being simple and intuitive, but do not provide any firm guarantees about the range of communication. Namely, an attacker with a strong enough transmitter and a high-gain antenna will still be able to communicate with the IMD even from far outside the intended range (for RFID-based solutions from up to ten meters away). Currently deployed solutions based on magnetic switches are equally based

on close-range communication; in addition they do not require any form of authentication to unlock access to the device and are thus inherently insecure (incidents were reported when pacemakers were unlocked by a magnetic field from a patient's headphones).

In this work, we propose a new access control mechanism for implantable medical devices. This mechanism is based on ultrasonic distance-bounding and enables an implanted medical device to grant access to its resources only to those devices that are in its close proximity. Our solution resembles close-range communication solutions proposed in prior work in that it requires a device to be close to the IMD to get access, but differs in that it prevents the attacker from accessing the IMD from further away, regardless of the type of transceiver or antenna he has. Its security relies on the speed of the sound which can not be altered. Moreover, unlike prior proposals, our solution enables IMDs to predefine an exact range from which they can be accessed (with a high degree of accuracy). We achieve this with a new proximity-based device pairing protocol based on ultrasonic distance bounding. In this protocol, messages are cryptographically tied to the distance bounds measured by the IMD, to the device that requests access. We analyze the security of our protocol in detail and discuss possible extensions related to efficiency and DoS protection.

We demonstrate the feasibility of our approach through experiments in an emulated patient environment. We show that, although implanted, IMDs can successfully verify the proximity of other devices. We further make new observations about the security of implementations of ultrasonic distance-bounding protocols. We show that without appropriate shielding of their ultrasonic circuitry, implementations of these protocols are vulnerable to attacks resulting from induced current in the audio receiver circuitry. We further show that given that our solution relies on ultrasonic distance-bounding, it can be implemented at low cost on existing IMD platforms (note that some pacemakers already come equipped with speakers).

Finally, we discuss the integration of our scheme with other solutions proposed for access to IMDs. We show that our solution can be easily combined with solutions based on security credentials or tokens as well as with solutions that aim to prevent battery draining Denial-of-Service attacks on IMDs. It also naturally integrates with solutions based on sonic user alerts. This work has been published at ACM CCS'09 [35].

- **Defending Embedded Systems Against Control Flow Attacks**

  We developped a control flow enforcement technique based on an Instruction Based Memory Access Control (IBMAC) implemented in hardware. It is specifically designed to protect low-cost embedded systems against malicious manipulation of their control flow as well as preventing accidental stack overflows. This is achieved by using a simple hardware modification to divide the stack in a data and a control flow stack (or return stack). Moreover access to the control flow stack is restricted only to return and call instructions, which prevents control flow manipulation. Previous solutions tackled the problem of control flow injection on general purpose computing devices and are rarely applicable to the simpler low-cost embedded devices, that lack for example of a Memory Management Unit (MMU) or execution rings. Our approach is binary compatible with legacy applications and only requires minimal changes to the tool-chain. Additionally, it does not increase memory usage, allows an optimal usage of stack memory and prevents accidental stack corruption at run-time. We have implemented and tested IBMAC on the AVR micro-controller using both a simulator and an implementation of the modified core on a FPGA. The implementation on reconfigurable hardware showed a small resulting overhead in terms of number of gates, and therefore a low overhead of expected production costs.

  This work was published at ACM SecureCode09 [25].

- **RFID Private Identification**

  We have been participating in the ANR RFID-AP project, and working on contactless card security and the security of embedded, low-cost cryptographic algorithms. We have been working with the community-driven OpenPCD contactless reader (for which we have submitted some patches).

Cryptography ensures the condentiality and authenticity of information but often relies on unproven assumptions. SAT solvers are a powerful tool to test the hardness of certain problems and have successfully been used to test hardness assumptions. This work extends a SAT solver to eciently work on cryptographic problems. The paper further illustrates how SAT solvers process cryptographic functions using automatically generated visualizations, introduces techniques for simplifying the solving process by modifying cipher representations, and demonstrates the feasibility of the approach by solving three stream ciphers. To optimize a SAT solver for cryptographic problems, we extended the solver's input language to support the XOR operation that is common in cryptography. To better understand the inner workings of the adapted solver and to identify bottlenecks, we visualize its execution. Finally, to improve the solving time signicantly, we remove these bottlenecks by altering the function representation and by pre-parsing the resulting system of equations. The main contribution of this work is a new approach to solving cryptographic problems by adapting both the problem description and the solver synchronously instead of tweaking just one of them. Using these techniques, we were able to solve a well-researched stream cipher 26 times faster than was previously possible.

This work has been published at SAT'09 [38].

- **Physical Layer Security**

  New approaches that generate secret keys from radio channels characteristics have been recently proposed. The security of these schemes usually relies on the reciprocity principle which states that the channel fluctuations can be a source of common randomness for two communicating peers and these fluctuations canât be measured by any eavesdropper. A validation of these properties for indoor environments is presented in this work. The shared keys are created by measuring the reciprocal channel features and converting this information to binary vectors using a quantization algorithm. This paper addresses the problem of quantization. It identifies an important weakness of existing key generation algorithms and it shows that the secret bits extraction has a significant impact on the robustness and security of these algorithms. A new adaptive quantization algorithm for secret key generation is presented. This method has the advantages to create sufficient long secret keys with a high key agreement ratio between authorized users without revealing information to the attacker. The new scheme is experimentally validated using Ultra Wide Band technology.

  This paper has been published at NTMS'09 [17].

- **Geolocalization of Hidden Servers**

  Cyber-crime is consolidating as a major threat for end users and infrastructures on the Internet. Criminals are employing ever changing and more sophisticated techniques to improve the effectiveness, reliability and stealthiness of their illegal activities. Entire underground infrastructures of compromised computers, called botnets, have bee n created to perform a wide range of illegal activities like sending unsolicited e-mail messages, identity theft, disrupting the availability of online services, etc.

  An emerging new use of botnets by cyber-criminals is a technique called fast-flux, which allows them to reliably host illegal content within a botnet. The study of these malicious networks by security researchers is made difficult by the use of encrypted and obfuscated communications between the participating nodes inside botnets. This calls for research in non-invasive network measurement techniques on botnets in order to understand the way they are used, possibly uncovering the motivations behind them.

  Recent promising proposals within the network community, provide ways to reveal either geographic coordinates or network virtual coordinates of Internet hosts. The general idea used to geolocalize Internet hosts is to consider a set of landmarks measuring network distances towards targets and then consider a model that represents a relationship between the geographic distance and the network measurements. Such model, once calibrated, is used by each landmark to derive a geographic distance towards the target, that is then located using multilateration.

  In this work, we extended the *Constraint-Based Geolocation* (CBG) technique to proxied communications, revealing in particular the geographic position of the roots of fast-flux networks. We perform

an experimental evaluation of the accuracy of localization in a controlled environment, using the PlanetLab infrastructure, where the exact location of targets is known. Our experimentations show promising results, with geolocalization accuracy similar or even better than non-proxied communication. In particular, we are able to localize hidden servers with mean error distance below $100\ km$. A vast majority of the obtained confidence zones, a zone where the target lies with a very high probability, allows for a resolution at the regional or even city level, similarly to the original non-proxied system.

In the light of these encouraging results, we tested our geolocalization approach in the wild and located several fast-flux servers. We then validated these results by infiltrating the Waledac fast-flux network to retrieve the IP addresses of some malicious servers.

This work has been published at ACM IMC'09 [20].

- **Cyber-Crime defenses and Botnets Study**

  While the Internet was probably one of the most important innovations of the past years, it is now commonly believed that it has reached its limits and a new architecture is required. Several researchers have already proposed to re-designe the Internet using a clean slate approach. One the reasons that is often cited is the lack of security of the current Internet. While the Internet is very reliable, it does not provide any build-in security mechanisms. It is advocated that the new Internet should be designed with security as one of the major requirements. I think this is a very interesting and exciting challenge. However, in order to achieve this goal, we should first have a clear understanding of today's security threats and how the Internet is used by cyber-criminals. Cyber-attacks are becoming more and more elaborated. Few years ago, the attacks were performed by script-kiddies that were just having fun. Nowadays, the attacks are performed by professionals that have very different motivations. These criminals are very innovative and use state-of the art technologies. One of the main threats today are botnets. A botnet is a network of compromised hosts on the Internet under the control of an attacker. They are used to send spams, performed Denial of Service attacks or collect/steal confidential data. Botnets account for more than 90% of all spams sent everyday.

  We have also recently set-up a new research activity on cyber-crime and botnet monitoring. We have studied a particular botnet, so called Storm. Storm uses a peer-to-peer protocol in order to coordinate the bots (the infected hosts) in the botnet. We have infiltrated Storm and were able to evaluate its size and study its malicious activities. Our study led to a great understanding of the inner workings of this botnet: how it is controlled, what kind of illegal activities are conducted with it, etc.

  In order to prevent the geo-localization of their malicious servers (phishing, illegal commercial servers), cyber-criminals usually use techniques based on proxies to hide the IP addresses of these machines. These proxies are usually compromized nodes (that are part of a botnet) and are changed very frequently, using a technique called "DNS Fax-fluxing". We are currently working on techniques to localize hidden servers. We showed that despite these re-direction mechanisms, it is still possible to geo-localize the malicious servers. We have then developed a tool that achieve such a geo-localization automatically.

  This work has been published in ACM IMC 2009 [20]

  The main goal of this research activity is to study how botnets actually work and how criminals operate. More generally, *we are aiming at understanding the underground economy and to contribute to the design of the Next Generation Internet*. This underground economy is very well structure and composed of many different actors. Some actors find vulnerabilities that are used by other actors to develop exploits. These exploits are then sold to other criminals that use them to compromise nodes and create botnets. These botnets are then rented for criminal activities (such as spamming, DoS attacks, extorsion and so on.).

- **Unstructured Overlay Security**

Recently, we have also been interested in the security of overlay networks. An overlay network is a virtual network formed by a subset of nodes in the underlying layer and virtual links composed of one or more hops on the lower-layer links. Recent research has shown a promising future for using application-layer overlay network to introducing new applications and services, e.g. multicast, resilient routing, peer-topeer file sharing, etc. However, no means exist today to perform large scale monitoring and anomaly detection in such networks. Although risks are common and attacks could be achieved by any legitimate user or an attackers that bypasses any authentication mechanisms. In this work, we have identified possible attacks on the overlay networks, and studied the impact of these attacks on the applications relying on these overlays. In a second step, we experimented with different classical traffic monitoring techniques to prove the inefficiency of the different application identification proposals (e.g. packet, flows, host aggregation techniques) when facing P2P-specific attacks. In a third step, we proposed to adopt a user-behavior identification technique to monitor overlay networks, and extend such monitoring to anomaly detection by designing a normal interaction model in such networks. This work has for now been published in [21]

- **Internet topology-inference security**

  We are also currently interested in Internet topology-inference security. So far, Internet measurements assumed the correct behavior of different entities that are participating in the measurements campaigns; However, since many malicious nodes may be involved into the measurements, we need to design robust-measurements techniques that would allow for an accurate and safe measurements of the Internet. We first illustrate this work by designing ways to hide path similarity exchanges among monitors that are exchanging sensitive topology data. In essence, the performance of several Internet applications often relies on the measurability of path similarity between different participants. In particular, the performance of content distribution networks mainly relies on the awareness of content sources topology information. It is commonly admitted nowadays that, in order to ensure either path redundancy or efficient content replication, topological similarities between sources is evaluated by exchanging raw traceroute data, and by a hop by hop comparison of the IP topology observed from the sources to the several hundred or thousands of destinations. In this work, based on real data we collected, we advocate that path similarity comparisons between different Internet entities can be much simplified and secured using lossy coding techniques, such as Bloom filters, to exchange compressed topology information. The technique we introduce to evaluate path similarity enforces both scalability and data confidentiality while maintaining a high level of accuracy. In addition, we demonstrate that our technique is scalable as it requires a small amount of active probing and is not targets dependent. This is an ongoing work we are actively investigating with the university of Louvain in Belgium and is under submissions [8].

- **Owner-Centric Networking**

  We are developing an 'owner-centric networking' architecture. This novel concept will considerably reduce 'data pollution' and improve privacy on the Internet. Content on the Internet (documents, emails, chats, images, videos etc) is often disseminated and replicated on different peers or servers. As a result, users lose the control and ownership of their content as soon as they release it.The crux of the problem is that the Internet simply never forgets, and information that is posted lingers virtually forever. Furthermore, the design of the current Internet places no limit on data diffusion, nor any right to an individual to modify or remove what he/she wrote on a forum chat, or on a famous social network's walls.

  This data pollution creates many privacy concerns, since this lost content can be used to collect information about users without their consent. For example, there have been several recent cases of employers using social networks (such as Facebook) to spy on their employees. The Internet of the Future should solve these data pollution and privacy problems. However, according to Schneier, "Privacy isn't something that occurs naturally online, it must be deliberately architected". More specifically, we argue that the future Internet should give individuals control over their data. Users should be able to retrieve their previously posted content in order to withdraw or modify it. In

other words, the Internet should enforce the 'right to forget', which is a constitutional law in several countries.

Unfortunately, most if not all future Internet architecture proposals seem to have ignored this issue so far. For example, the content-centric networking (CCN) architecture, which proposes that the focus be shifted from transmitting data by geographic location to disseminating it via named content, actually increases data pollution. In CCN, content is not only hosted by servers but also diffuses from its point of creation to where the consumers are. As a result, individuals completely lose control over their content as it becomes distributed (lost) on the Internet without their consent or even knowledge.

That said, we believe that content-centric networking is still a very attractive solution, if it then evolves towards an owner-centric architecture (OCN) that considers content ownership as bedrock. We have proposed the OCN architecture that gives control back to the users over their data.

This work has been published at ERCIM News [14] and FIST'09 [19].

6.3. Network measurement, modeling and understanding

Participants: Chadi Barakat, Walid Dabbous, Roberto Cascella, Alfredo Grieco, Mohamad Jaber, Amir Krifa, Imed Lassoued, Stevens Leblond, Arnaud Legout.

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 fast increase in Internet traffic and growth of its size. We propose solutions for a fast and accurate identification of Internet traffic based on packet size statistics. 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 to users by a better management of network resources and by a more efficient tuning of applications that take into account the constraints posed 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. This is the main functionality provided by our open-source software BitHoc [49].

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

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

  One of the most important challenges for network administrators is the identification of applications behind the Internet traffic. This identification serves for many purposes as in network security, traffic engineering and monitoring. The classical methods based on standard port numbers or deep packet inspection are unfortunately becoming less and less efficient because of encryption and the utilization of non standard ports. In this activity, we come up with an online iterative probabilistic method that identifies applications quickly and accurately by only using the size of packets. Our method associates a configurable confidence level to the port number carried in the transport header and is able to consider a variable number of packets at the beginning of a flow. By verification on real traces we observe that even in the case of no confidence in the port number, a very high accuracy can be obtained for well known applications after few packets were examined. Further details on the method and the experimental results can be found in [28]. The work is continuing by validating the method on more traces and extending its application to more advanced scenarios.

- **Adaptive network-wide traffic monitoring** The remarkable growth of the Internet infrastructure and the increasing heterogeneity of applications and users' behavior make more complex the manageability and monitoring of ISP networks and raises the cost of any new deployment. The main consequence of this trend is an inherent disagreement between existing monitoring solutions and the increasing needs of management applications. In this context, we work on the design

of an adaptive centralized architecture that provides visibility over the entire network through a network-wide cognitive monitoring system. Given a measurement task, the proposed system drives its own configuration 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. The performance of our system is being validated in typical scenarios over an experimental platform we are developing for the purpose of the study. This platform presents a new approach for the emulation of Internet traffic and for its monitoring across the different routers. It puts at the disposal of users a real traffic emulation service coupled to a set of libraries and tools capable of Cisco NetFlow data export and collection, the overall destined to run advanced applications for network-wide traffic monitoring and optimization.

The activities in this direction are funded by the ECODE FP7 STREP project (Sep. 2008 - Sep. 2011).

- **Spectral analysis of packet sampled traffic** Packet sampling techniques introduce measurement errors that should be carefully handled in order to correctly characterize the network behavior. In the literature several works have studied the statistical properties of packet sampling and the way it should be inverted to recover the original network measurements. Here we take the new direction of studying the spectral properties of packet sampling. A novel technique to model the impact of packet sampling is proposed based on a theoretical analysis of network traffic in the frequency domain. Moreover, a real-time algorithm is also developed to detect the spectrum portion of the network traffic that can be restored once packet sampling has been applied. The analysis and some experimental results to validate the approach are published in [26].
- **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.
- **Understanding peer-to-peer dynamics**

  This activity focuses on the understanding and improvement of peer-to-peer content delivery. Indeed, we believe that the value of peer-to-peer comes from its ability to distribute contents to a large number of peers without any specific infrastructure, and within a delay that is logarithmic with the number of peers.

  We have also worked, in the context of the Ph.D. thesis of Stevens Le Blond, on how to make BitTorrent ISP friendly [54]. One major issue with BitTorrent is that is does no take into account the

underlying network topology. As a consequence some specific links are overloaded, and ISPs have to block BitTorrent traffic in order to decrease the load on those links. One solution to this problem is keep the BitTorrent traffic local to each ISP, leveraging on the ISPs network topology. This notion of locality has raised a huge interest recently. However, all proposed solutions consider only moderate locality. In [54] we answer two important questions.

First, how much traffic can be kept local without adversely impacting peers? Whatever the locality solution is, it will impact the structure of the overlay interconnecting peers. We go much further than previous work on the understanding of the impact of locality on the structure of that overlay. In addition, reducing the amount of traffic that is kept local in order to prevent partitions (thus a loss of performance for peers) is the solution adopted by P4P and Ono. We introduce a simple mechanism (that is backward compatible) to prevent partitions and show that the traffic reduction on specific links can be dramatically reduced by keeping more traffic local without adversely impacting peers. Those kind of mechanisms are very important because they enable to reap full benefits from the information provided by the locality solution.

Second, what would be the benefit of a locality policy at the Internet scale? We show using a real world crawl of a large fraction of the all BitTorrent peers that the benefit from deploying a locality policy today would be a reduction of 40% on inter-AS links. To the best of our knowledge, the work closer to ours is the one of P4P. However, they only consider one torrent and one AS. Whereas the P4P field tests are successfully used to support the relevance of the P4P architecture, they cannot be used to support the relevance of a locality policy at the scale of the Internet. But that last point fundamental for the locality justification. A classical argument is that at the scale of the Internet the benefit of a locality policy will be negligible because there is on average one or a few peers per AS. We show that even if it is true that there is on average few peers per AS, the reduction of traffic on inter-AS links that can be achieved using a locality policy is still high at the Internet scale. Thus we believe that this is the first large scale measurement that strongly support the relevance of the implementation of a locality policy in the Internet.

In another work [57], we evaluate the experimental bias that may occur when running BitTorrent experiments on a testbed. We show that there is no bias due to the shorter delay compared to the real internet. Therefore, it means that very realistic BitTorrent experiments can be run on a testbed or cluster of machines.

Finally, we have explored privacy issues with BitTorrent. In a first work, we show for the first time that it is possible to monitor in real time all peers that are using BitTorrent world wide. Using this information, we show that the initial source of contents can be identified and we quantified their impact on the performance of BitTorrent.

In a Second work, we show that TOR, the anonymizing network, fails to protect the privacy of BitTorrent users. Indeed, we show that it is possible the retreive the IP address of BitTorrent users on top of Tor, but even worse, that all applications run by those users are potentially compromized.

6.4. Experimental Environment for future Internet architecture

Participants: Walid Dabbous, Diego Dujovne, Martin Ferrari, Mads Hansen, Mathieu Lacage, Thierry Parmentelat, Alina Quereilhac, Bilel Ben Romdhanne, Thierry Turletti, Shafqat Ur Rehman.

- **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. Wire-

less 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 packets trace storage. This solution reduces processing time by 400space by 200% with regard to raw trace files solutions [43]. 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.

- **Enhancing network simulations: the ns-3 simulator**

  Our main problem with existing simulation tools is the lack of accuracy of the application, network, and MAC/PHY layers which makes comparisons with real-world experimentations very hard, if not impossible. The core of the issue is that none of the existing network simulators allow easy re-use of existing real-world network components such as the TCP/IP stacks of an operating system together with a real-world routing protocol and a full 802.11 MAC layer.

  Our involvement in the development of ns-3 focused on 3 major areas last year: the stabilization of its core architecture and facilities for its first stable releases, incremental improvements of our wimax models, and the development of a POSIX implementation to allow us to run unmodified socket-based network applications within the simulator.

  After the first stable release of ns-3 in 2008 and the merging of our wifi, and icmp models, we kept working on both general software maintainance activities (code reviews of new models, bug fixing, release management) but also on improvements to our wimax models which we hope to merge in ns-3 in early 2010 (see description hereafter). We also invested considerable efforts in two other projects which we aim to merge in ns-3 over the course of 2010:

  – the development of a new parallel event scheduler for multicore shared-memory architectures to speedup simulations transparently
  – an implementation of the POSIX API within ns-3 to integrate bit-torrent clients and trackers, but also the reference CCN daemon and test applications.

  With the recent emergence of broadband wireless networks, simulation support for such networks, and especially IEEE 802.16 WiMAX, is becoming a necessity. 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 fundamental functions of the convergence sublayer (CS) and the MAC common-part sublayer (CPS), including QoS scheduling services, bandwidth request/grant mechanism, and a simple uplink scheduler. The module provides two different versions of the PHY layer. The first one is a basic PHY implementation which simply forwards bursts received by the MAC layer ignoring any underlying PHY layer details. The second one is a PHY layer based on the WirelessMAN-OFDM specification and was developed by our colleagues at LIP6, France. The MAC module currently lacks a full implementation of the classifier as well as support for fragmentation and defragmentation of PDUs. The simulation module is described in [24].

- **Federating Research Testbeds**

  In cooperation with Princeton University who run the PlanetLab research platform, we have developped the first prototype of a federation paradigm called RefreshPeer (RP), that provides a fully symetric model, where resources are locally managed and globally visible. This mechanism was designed with operational objectives in mind, as it was a requirement for the OneLab project to operate the new PlanetLab Europe platform, that has been running since June 2007. There are thus some

limitations in this first prototype, that are related to policy management and scalability. This federation model basically relies on database caching; essentially the API that each testbed infrastructure (peer) provides has been kept unchanged except for convenience and efficiency, and it was shown to be sufficient to this particular need. This year, the main focus has been on development, testing and experimental deployment of a relatively new network testbed federation mechanism called SFA (Slice based Facility Architecture). This work is being done in collaboration with the Computer Science department of Princeton University. We started by developing SFA on top of the PlanetLab testbed architecture to enable federation among multiple autonomous instance of PlanetLabs. We then enhanced SFA with essential features such as call traceability and logging to track user activities in the context of multiple federated aggregates. We also developed a code base to ensure that SFA is compatible with RefreshPeer (RP), the federation mechanism we have developed before and the only mechanism that was in existence prior to SFA and still actively in use for federation between PlanetLab Europe (PLE) and PlanetLab Central (PLC). The objective is to enable both RP and SFA based federation between PLE and PLC to take advantage of these two mechanism. We then installed SFA on PLE nodes and we made the necessary configuration for federation with PLC Finally we developed an automatic test framework to test SFA as part of the nightly build of Onelab. The SFA software is now packaged and distributed along with Onelab distribution of MyPLC.

- **Adding more heterogeneity to the PlanetLab testbed**

  As part of the OneLab project, we have created our own 'distribution' of the PlanetLab software, and have used the flexibility in order to add support for more heterogeneous experimental nodes, like wireless (WiFi, UMTS) or multi-homed nodes. Over time, the software development cooperation with Princeton University has moved from an upstream/downstream model to codevelopment. As a result, most of our contribution is expected was integrated in the 4.2 and 4.3 releases of the PlanetLab software.

- **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 [44]. The development of NEPI started in early 2009 with the implementation of the core API, an address allocator, a routing table configurator, but also a prototype ns-3 backend driven by a simple graphical user interface based on QT. In 2010, we expect to validate and evolve the core API with the addition of a new backend based on linux network namespace containers and to stabilize the existing ns-3 backend. These first two milestones will be followed 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.

7. Contracts and Grants with Industry

7.1. Industrial contracts

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 supports Amine Ismail.

8. Other Grants and Activities

8.1. National projects

RNRT C'MON (2009-2012):
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 company. CMON stands for collaborative monitoring. It is an industrial research project that will develop the technology needed to allow end-users to collaborate in order to identify the origin and cause of Internet service degradation. The main differentiating assumptions made in this project are that (i) ISPs do not cooperate together, and (ii) one cannot rely on any information they provide in order to diagnose service problems. Even more, CMON considers that these ISP will try to masquerade the user observations in order to make their service look better. The software designed in this project will be added to the toolbox currently provided by the Grenouille project. The hope is that such a project will encourage ISPs to improve their quality of service and will contribute to improve customer satisfaction.

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/Minalogic SHIVA (2009-2012):
The goal of the SHIVA project (Secured Hardware Immune Versatile Architecture) is to design a high performance security gateway, using a high performance re-programmable and reconfigurable security FPGA board, plugged in a commodity PC. The INRIA Moais and INRIA Planète team both participate, jointly, to this project leaded by CS-SI.

ANR/RNRT CAPRI-FEC (2007-2009):
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 are INRIA (leader), CEA-LETI, ENSICA, STMicroelectronics, and (NAME REMOVED).

ANR/CIS HIPCAL (2007-2009):
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.

Industrial contract with (NAME REMOVED) (2008-2011):
The goal of this study the use of AL-FEC techniques in broadcasting systems.

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.

8.2. European projects

OneLab (2006-2010) :
OneLab has be 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 to "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.

ITEA Expeshare (2007-2009):
Expeshare is an ITEA project to enable virtual communities to share media experiences in their personal devices legally and securely. The final aim is to develop and implement an architecture for a wireless peer-to-peer network that links personal devices and realizes DRM and mobile payment functionality and allows for legal and secure sharing of multimedia content and experiences. Over 25 European partners are involved mainly Philips, Nokia, Telefonica, VTT, the GET-INT and the university of Evry. The role of INRIA in this project is to participate to the design and evaluation of protocols for the network and Peer-to-Peer layer in order to support the sharing of media in a wireless network. We are studying the feasibility of running actual Peer-to-Peer solutions over wireless networks and trying to understand their limitations. Based on that, we are proposing new solutions to efficiently localize resources in a wireless network and to share it with other interested users. The propositions made by INRIA will be the subject of integration to modules proposed by other partners and extensive evaluation by simulation and real experimentations. The BitHoc software [49] gives an idea on our contribution within Expeshare.

FP7 STREP ECODE (2008-2011):
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 measurement task 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.

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.

IST STREP UbiSec&Sens (2006-2009):
PLANETE is part of the IST UbiSec&Sens project. The goal of this project is to develop new security protocols for wireless sensor networks. The follow-up of this project, called WSN4CIP, started on january 2009. It goal is to provide solutions that use WSN to protect Critical Infrastructures.

8.3. INRIA supported Activities

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

Rapid advances in microelectronics are making it possible to mass-produce tiny inexpensive devices, such as processors, RF-IDs, sensors, and actuators. These devices are already, or soon will be, deployed in many different settings for a variety of purposes, which typically involve tracking (e.g., of hospital patients, military/rescue personnel, wildlife/livestock and inventory in stores/warehouses) or monitoring (e.g., of seismic activity, border/perimeter control, atmospheric or oceanic conditions). In fact, it is widely believed that, in the future, sensors will permeate the environment and will be truly ubiquitous in clothing, cars, tickets, food packaging and other goods.

These new highly networked environments create many new exciting security and privacy challenges. The objectives of the UbiSec associated team is to understand and tackle some of them. More specifically, the proposed project will consider the following three topics: 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.

Roseate (STIC AmSud): This project (2008-2009) 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.

ADT PLECS: This project (2008-2010) 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.

9. Dissemination

9.1. Promotion of the Scientific Community

Walid Dabbous served in 2009 as PC member in ICC'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 ubinet.inria.fr). He also served as an expert to the European Commission to evaluate EC funded projects.

Claude Castelluccia served in 2009 in the program committees of the following international conferences: 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 IEEE member, is in the Program Committee of the following conferences/workshops: Packet Video'09, the 2nd International Workshop on mobile Video Delivery (Movid)'09. 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 since 2005. In 2009, he served on the Technical Program Committee for several conferences as Infocom 2009, Algotel 2009, ITC 2009. Chadi Barakat was invited to give talks at different places as ETH (Zurich), Bell-Labs (NJ).

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).

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.

9.2. University Teaching

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

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

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

Wireless networking: 7h, Master RTM, IUP Avignon, 2009, by C. Barakat.

Local Aarea Networks: 21 hours course + 10.5 hours practical work, IUT of the University of Nice-Sophia Antipolis, 2007-2010, by C. Barakat.

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

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).

Networks: Undergraduate course at University of Nice-Sophia Antipolis, by C. Barakat (6h).

Peer-to-peer networks: Course in the UbiNet master at University of Nice-Sophia Antipolis 2009 (15h), by Arnaud Legout

Networks and Telecommunications: Programming Courses given to the students of the Ensimag, Grenoble by Mohamed Ali Kaafar (18h).

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

9.3. PhD Theses and Internships

9.3.1. HDR defended in 2009

1. Chadi Barakat defended his accreditation to supervise research (HDR) on January 2009 [1]. The title of his HDR thesis is "Solutions efficaces pour la métrologie de l'Internet".

9.3.2. PhDs defended in 2009

1. Diego Dujovne has defended his PhD in May 2009. He worked on "Enhancing Experimentation in Wireless Networks" [2].
2. Aurélien Francillon defended his PhD in October 2009. He worked on "Attacking and Protecting Constrained Embedded Systems from Control Flow Attacks" [3].
3. Mate Soos defended his PhD in October 2009. He worked on "Privacy-preserving Security Protocols for RFIDs" [4].

9.3.3. Ongoing PhDs

1. Sana Ben Hamida works on "Embedded System Security".
2. Mathieu Cunche works on "Forward Error correction codes for the erasure channel ".
3. Diego Dujovne works on "Wireless Experimental Test-beds".
4. Aurélien Francillon works on "WSN security".
5. Amine Ismail works on "Optimisation of IP Protocols and Applications over Broadcast Links".
6. Mohamad Jaber works on "Detection and Troubleshooting of Internet Anomalies".
7. Mathieu Lacage works on "An IP-level network topology and link characteristic measurement tool".
8. Imed Lassoued works on "Adaptive Sampling".
9. Stevens Le Blond works on "Next Generation Peer-to-Peer Infrastructures".
10. Pere Manils works on "Security of the TOR network".
11. Daniele Perito works on "Critical Infrastructure Protection".

12. Naveed Bin Rais works on “Adaptive Communication Mechanisms for Networks with Episodic Connectivity”.
13. Mohamed Karim Sbai works on “Architecture for data sharing in wireless network”.
14. Mate Soos works on“RFID Security”.
15. Shafqat Ur Rehman works on “‘Benchmarking Methodology for Network Protocols Evaluation”.

9.3.4. Training activities

1. Emiliano De Cristofaro worked on an Internet Privacy project. Duration of the stay: 4 months. Prepared degree: Phd Degree in Computer Science. Affiliation: University of California, Irvine.
2. Abdelberi Chaabane worked on Unstructured Overlay Security. Duration of the stay: 6 months. Prepared degree: Master Thesis in Computer Science. Affiliation: ENSI, University of Manouba, Tunisia.
3. Giuseppe PIRO worked on Optimising WiMax scheduling algorithms for the ns-3 simulator. Duration of the stay: 2 months. Prepared degree: PhD. Affiliation: Politechnico di Bari, Italy.
4. Martin Hernan Ferrari worked on Using Independent Simulators, Emulators, and Testbeds for Easy Experimentation. Duration of the stay: 6 months. Affiliation: Buenos Aires University.
5. Cao Cuong GNO worked on Internet monitoring via active probes on PlanetLab. Duration of the stay: 6 months. Prepared degree: Master. Affiliation: Institut de la Francophonie pour l’Informatique, Hanoi, Viet Nam.
6. Ludovic Fardel worked on Content distribution infrastructure. Duration of the stay: 6 months. Prepared degree: EPFL Engineer. Affiliation: EPFL, Lausanne, Swtizerland.
7. Guillaume Séguin worked on Multicore Network Simulation. Duration of the stay: 2 months and a half. Prepared degree: Computer Science degree at Ecole Normale Supérieure. Affiliation: ENS Ulm, Paris.
8. Mariem Abdelmoula worked on Simulation of the IEEE 802.16 WiMax Packet CS convergence layer. Duration of the stay: 4 months. Prepared degree: Engineering diploma. Affiliation: Supcom, Tunisia.
9. Maher Ben Yahmed worked on Validation with experimentation if innovative MAC mechanisms for WiFi. Duration of the stay: 4 months. Prepared degree: Engineering diploma. Affiliation: ENSI, Tunisia.
10. Marcel Sutter worked on New Services for the Internet. Duration of the stay: 5 months. Prepared degree: Engineering diploma. Affiliation: EPFL, Lausanne, Switzerland.
11. Adrien Gallais worked on the deployment of a wireless experimental platform. Duration of the stay: one month and a half. Prepared degree: Engineering diploma. Affiliation: Ecole Centrale d’Electronique, Paris.
12. Gaël Grimaud worked on the deployment of a wireless experimental platform. Duration of the stay: 2 months. Prepared degree: DUT. Affiliation: University of Nice Sophia Antipolis.

10. Bibliography

Year Publications

Doctoral Dissertations and Habilitation Theses

[1] C. BARAKAT. *Solutions efficaces pour la métrologie de l’Internet*, Université de Nice Sophia Antipolis, 01 2009, http://tel.archives-ouvertes.fr/tel-00408745/en/, Habilitation à Diriger des Recherches.

[2] D. DUJOVNE. *Amélioration des expérimentations sur réseaux sans fil*, Université de Nice Sophia Antipolis, 05 2009, http://tel.archives-ouvertes.fr/tel-00408682/en/, Ph. D. Thesis.

[3] A. FRANCILLON. *Attacking and Protecting Constrained Embedded Systems from Control Flow Attacks*, INPG, October 2009, PhD thesis.

[4] M. SOOS. *Privacy-preserving Security Protocols for RFIDs*, INPG, October 2009, PhD Thesis.

Articles in International Peer-Reviewed Journal

[5] C. CASTELLUCCIA, A. CHAN, E. MEYKLETUN, G. TSUDIK. *Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks*, in "ACM ToSN (Transaction on Sensor Networks)", 2009.

[6] R. DI PIETRO, L. V. MANCINI, C. SORIENTE, A. SPOGNARDI, G. TSUDIK. *Data Security in Unattended Wireless Sensor Networks*, in "Autonomic Network Computing, IEEE Transaction on Computers", 2009.

[7] B. DONNET, B. GUEYE, M. A. KAAFAR. *A survey on Network Coordinates Systems, Design and Security*, in "IEEE Communications Surveys and Tutorials", 2009.

[8] B. DONNET, B. GUEYE, M. A. KAAFAR. *Path Similarity Evaluation Using Bloom Filters*, in "Computer Networks, The International Journal of Computer and Telecommunications Networking", 2009.

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

[10] MOHAMED HOSSEIN. MANSHAEI, M. LACAGE, C. HOFFMANN, T. TURLETTI. *On Selecting the Best Transmission Mode for WiFi Devices*, in "Wireless Communications and Mobile Computing", vol. 9, n^{o} 7, July 2009.

[11] S. PETER, D. WESTHOFF, C. CASTELLUCCIA. *A Survey on the Encryption of Convergecast-Traffic with In-Network Processing*, in "IEEE Transactions on Dependable and Secure Computing (TDSC)", 2009.

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

[13] T. SPYROPOULOS, T. TURLETTI, K. OBRACZKA. *Routing in Delay Tolerant Networks Comprising Heterogeneous Node Populations*, in "IEEE Transaction on Mobile Computing", vol. 8, n^{o} 8, August 2009.

Articles in Non Peer-Reviewed Journal

[14] C. CASTELLUCCIA, MOHAMED ALI. KAAFAR. *Owner-Centric Networking: A New Architecture for a Pollution-Free Internet*, in "ERCIM News, Special Theme on Future Internet Technology", vol. 77, 2009, http://ercim-news.ercim.org/images/stories/EN77/EN77-web.pdf.

International Peer-Reviewed Conference/Proceedings

[15] A. AL-HAMRA, N. LIOGKAS, A. LEGOUT, C. BARAKAT. *Swarming Overlay Construction Strategies*, in "Proceedings of ICCCN 2009, San Francisco, CA, USA", 2009, http://hal.inria.fr/inria-00385351/en/LBUS.

[16] A. ALLOUM, B. SAYADI, V. ROCA. *Reed Solomon Codes On Graph for DVB-SH Streaming Services*, in "22nd Wireless World Research Forum (WWRF'09), Paris, France", 2009, http://hal.inria.fr/inria-00390693/en/.

[17] S. BENHAMIDA, J. PIERROT, C. CASTELLUCCIA. *An Adaptive Quantization Algorithm for Secret Key Generation using Radio Channel Measurements*, in "International Conference on New Technologies, Mobility and Security (NTMS)", Dec. 2009.

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

[19] C. CASTELLUCCIA, MOHAMED ALI. KAAFAR. *Owner-Centric Networking (OCN): Toward A Data Pollution-Free Internet*, in "SAINT Workshop on Trust and Security in the Future Internet, FIST, Seattle, USA", IEEE Communications Society, July 2009.

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

[21] A. CHAABANE, MOHAMED ALI. KAAFAR. *Revisiting unstructured overlay network security*, in "Foundations and Practice Of Security workshop, Grenoble", June 2009.

[22] M. CUNCHE, V. ROCA. *Adding Integrity Verification Capabilities to the LDPC-Staircase Erasure Correction Codes*, in "IEEE Global Communications Conference (GLOBECOM 2009)", November 2009.

[23] M. CUNCHE, V. ROCA. *Le RFC 5170 en pratique : conception et évaluation d'un codec AL-FEC LDPC-staircase hautes performances*, in "Colloque Francophone sur l'Ingénierie des Protocoles (CFIP)", October 2009.

[24] J. FAROOQ, T. TURLETTI. *An IEEE 802.16 WiMAX Module for the NS-3 Simulator*, in "ICST Simutools, Roma, Italy", March 2009.

[25] A. FRANCILLON, D. PERITO, C. CASTELLUCCIA. *Defending embedded systems against control flow attacks*, in "SECUCODE'09: 1st ACM wokshop on secure code execution", Nov. 2009.

[26] L. A. GRIECO, C. BARAKAT. *An Analysis of Packet Sampling in the Frequency Domain*, in "proceedings of the ACM Internet Measurement Conference (IMC), Chicago", November 2009.

[27] MOHAMED AMINE. ISMAIL, T. TURLETTI, W. DABBOUS. *Optimizing the DVB-SH FEC Scheme for Efficient Erasure Recovery*, in "Mobile Video Delivery (MOVID) Workshop at Infocom, Rio de Janeiro, Brazil", April 2009.

[28] M. JABER, C. BARAKAT. *Enhancing Application Identification By Means Of Sequential Testing*, in "proceedings of IFIP/TC6 Networking Conference, Aachen, Germany", May 2009.

[29] M. A. KAAFAR, F. CANTIN, B. GUEYE, G. LEDUC. *Detecting Triangle Inequality Violations for Internet Coordinate Systems*, in "Proceedings of International Workshop on the Network of the Future", June 2009.

[30] M. A. KAAFAR, L. MATHY, C. BARAKAT, K. SALAMATIAN, T. TURLETTI, W. DABBOUS. *Certified Internet Coordinates*, in "proceedings of IEEE ICCCN conference, San Francisco", August 2009.

[31] A. KRIFA, K. SBAI, C. BARAKAT, T. TURLETTI. *A standalone content sharing application for spontaneous communities of mobile handhelds*, in "demo description in proceedings of the ACM SIGCOMM MobiHeld Workshop, Barcelona", August 2009.

[32] A. KRIFA, K. SBAI, C. BARAKAT, T. TURLETTI. *BitHoc: A content sharing application for Wireless Ad hoc Networks*, in "demo description in proceedings of the IEEE Percom conference, Galveston, Texas", March 2009.

[33] S. LE BLOND, F. LE FESSANT, E. LE MERRER. *Finding Good Partners in Availability-aware P2P Networks*, in "International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'09), Lyon, France", 2009, http://hal.inria.fr/inria-00432741/en/.

[34] Y. LIAO, MOHAMED ALI. KAAFAR, B. GUEYE, F. CANTIN, P. GEURTS, G. LEDUC. *Detecting Triangle Inequality Violations in Internet Coordinate Systems by Supervised Learning*, in "Proceedings of the IFIP Networking Conference 2009", May 2009.

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

[36] K. SBAI, C. BARAKAT. *Revisiting content sharing in wireless ad hoc networks*, in "proceedings of the fourth workshop on self-organizing systems (IWSOS), Zurich", December 2009.

[37] K. SBAI, E. SALHI, C. BARAKAT. *A membership management protocol for mobile P2P networks*, in "proceedings of the ACM Mobility Conference, Nice", September 2009.

[38] M. SOOS, K. NOHL, C. CASTELLUCCIA. *Extending SAT solvers to cryptographic problem*, in "International Conference on Theory and Applications of Satisfiability Testing (SAT)", jul 2009.

[39] A. SORO, M. CUNCHE, J. LACAN, V. ROCA. *Erasure Codes with a Banded Structure for Hybrid Iterative-ML Decoding*, in "IEEE Global Communications Conference (GLOBECOM 2009)", November 2009.

[40] P. VICAT-BLANC PRIMET, V. ROCA, J. MONTAGNAT, JEAN-PATRICK. GELAS, O. MORNARD, L. GIRAUD, G. KOSLOVSKI, T. TRUONG HUU. *A Scalable Security Model for Enabling Dynamic Virtual Private Execution Infrastructures on the Internet*, in "9th IEEE International Symposium on Cluster Computing and the Grid (CCGrid'09), Shanghai, China", May 2009.

National Peer-Reviewed Conference/Proceedings

[41] S. LE BLOND, F. LE FESSANT, E. LE MERRER. *Choix de partenaires en p2p suivant des critères de disponibilité*, in "conférence francaise sur les systèmes d'exploitation, Toulouse, France", 2009, http://hal.inria.fr/inria-00432747/en/.

[42] E. SALHI, M. K. SBAI, C. BARAKAT. *Neighborhood selection in mobile P2P networks*, in "Algotel, Carry-Le-Rouet, France", A. CHAINTREAU, C. MAGNIEN (editors), 2009, http://hal.inria.fr/inria-00383344/en/.

Workshops without Proceedings

[43] B. BEN ROMDHANNE, D. DUJOVNE, T. TURLETTI. *Efficient and Scalable Merging Algorithms for Wireless Traces*, in "Proceedings of the 4th ROADS Workshop, Montana, USA", October 2009.

[44] M. LACAGE, M. FERRARI, M. HANSEN, T. TURLETTI. *NEPI: Using Independent Simulators, Emulators, and Testbeds for Easy Experimentation*, in "Proceedings of the 4th ROADS Workshop, Montana, USA", October 2009.

Research Reports

[45] C. BARAKAT, K. SBAI, A. DECREME. *TICP: Transport Information collection Protocol*, 2009, http://planete.inria.fr/ticp/.

[46] B. BEN ROMDHANNE, D. DUJOVNE, T. TURLETTI, W. DABBOUS. *Efficient and scalable merging algorithms for wireless traces*, INRIA, 2009, http://hal.inria.fr/inria-00397832/en/, RR-6969, Rapport de recherche.

[47] M. CUNCHE, V. ROCA. *Adding Integrity Verification Capabilities to the LDPC-Staircase Erasure Correction Codes*, INRIA, 2009, http://hal.inria.fr/inria-00379155/en/, Technical report.

[48] M. CUNCHE, V. ROCA. *Le RFC 5170 en pratique : conception et évaluation d'un codec AL-FEC LDPC-staircase hautes performances*, INRIA, 2009, http://hal.inria.fr/inria-00386166/en/, Rapport de recherche.

[49] A. KRIFA, K. SBAI, C. BARAKAT, T. TURLETTI. *BitHoc: BitHoc: Tracker-less BitTorrent for Mobile Ad Hoc Networks*, 2009, http://planete.inria.fr/bithoc/.

[50] M. LACAGE, M. FERRARI, M. HANSEN, T. TURLETTI, W. DABBOUS. *NEPI: Using Independent Simulators, Emulators, and Testbeds for Easy Experimentation*, INRIA, 2009, http://hal.inria.fr/inria-00397692/en/, RR-6967, Rapport de recherche.

[51] J. LACAN, E. LOCHIN, P.-U. TOURNOUX, A. BOUABDALLAH, V. ROCA. *On-the-fly coding for time-constrained applications*, Computing Research Repository, April 2009, http://www.citebase.org/abstract?id=oai:arXiv.org:0904.4202, Research Report.

[52] J. LACAN, V. ROCA, J. PELTOTALO, S. PELTOTALO. *Reed-Solomon Forward Error Correction (FEC) Schemes*, April 2009, IETF Request for Comments, RFC 5510 (Standards Track/Proposed Standard).

[53] S. LE BLOND, F. LE FESSANT, E. LE MERRER. *Finding Good Partners in Availability-aware P2P Networks*, INRIA, 2009, http://hal.inria.fr/inria-00352529/en/, RR-6795, Rapport de recherche.

[54] S. LE BLOND, A. LEGOUT, W. DABBOUS. *Pushing BitTorrent Locality to the Limit*, INRIA, 2009, http://hal.inria.fr/inria-00343822/en/, Technical report.

[55] S. LE BLOND, P. MANILS, A. CHAABANE, M. A. KAAFAR, A. LEGOUT, C. CASTELLUCCIA. *De-anonymizing BitTorrent Users on Tor*, INRIA, December 2009, Technical report.

[56] J.-C. MAUREIRA, D. DUJOVNE, O. DALLE. *Network Provisioning for High Speed Vehicles Moving along Predictable Routes - Part 1: Spiderman Handover*, INRIA, 2009, http://hal.inria.fr/inria-00369419/en/, RR-6850, Rapport de recherche.

[57] A. RAO, A. LEGOUT. *Impact of Network Latencies on the Outcome of BitTorrent Experiments Performed on Testbeds*, INRIA, December 2009, Technical report.

[58] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, March 2009, IETF RMT Working Group (individual document), Work in Progress: <draft-roca-rmt-newfcast-04.txt>.

[59] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, July 2009, IETF RMT Working Group (individual document), Work in Progress: <draft-roca-rmt-newfcast-05.txt>.

[60] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, October 2009, IETF RMT Working Group (individual document), Work in Progress: <draft-roca-rmt-newfcast-05.txt>.

[61] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Reed-Solomon Forward Error Correction (FEC) Schemes for FECFRAME*, July 2009, IETF FECFRAME Working Group, Work in Progress: <draft-roca-fecframe-rs-01.txt>.

[62] V. ROCA, M. CUNCHE, J. LACAN, A. BOUABDALLAH, K. MATSUZONO. *Reed-Solomon Forward Error Correction (FEC) Schemes for FECFRAME*, March 2009, IETF FECFRAME Working Group, Work in Progress: <draft-roca-fecframe-rs-00.txt>.

[63] V. ROCA, M. CUNCHE, J. LACAN. *LDPC-Staircase Forward Error Correction (FEC) Schemes for FECFRAME*, July 2009, IETF FECFRAME Working Group, Work in Progress: <draft-roca-fecframe-ldpc-00.txt>.

[64] V. ROCA, A. FRANCILLON, S. FAURITE. *TESLA source authentication in the ALC and NORM protocols*, September 2009, IETF RMT Working Group, Work in Progress: <draft-msec-tesla-for-alc-norm-08.txt>.

[65] V. ROCA, A. FRANCILLON, S. FAURITE. *TESLA source authentication in the ALC and NORM protocols*, October 2009, IETF RMT Working Group, Work in Progress: <draft-msec-tesla-for-alc-norm-09.txt>.

[66] V. ROCA, A. FRANCILLON, S. FAURITE. *TESLA source authentication in the ALC and NORM protocols*, October 2009, IETF RMT Working Group, Work in Progress: <draft-msec-tesla-for-alc-norm-10.txt>.

[67] V. ROCA. *Simple Authentication Schemes for the ALC and NORM Protocols*, March 2009, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-simple-auth-for-alc-norm-01.txt>.

[68] M. K. SBAI, C. BARAKAT. *Revisiting content sharing in wireless ad hoc networks*, INRIA, 2009, http://hal.inria.fr/inria-00376521/en/, Rapport de recherche.

[69] A. SORO, M. CUNCHE, J. LACAN, V. ROCA. *Erasure Codes with a Banded Structure for Hybrid Iterative-ML Decoding*, Computing Research Repository, January 2009, http://www.citebase.org/abstract?id=oai:arXiv.org:0901.3467, Research Report.