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 COM

Activity Report

2007

Table of contents

1. Team

Head of project-team

Walid Dabbous [DR, Inria]

Vice-head of project-team in Grenoble

Claude Castelluccia [DR, Inria]

Vice-head of project-team in Sophia

Thierry Turletti [CR, Inria, HdR]

Research scientists

Chadi Barakat [CR, Inria]
Arnaud Legout [CR, Inria]
Vincent Roca [CR, Inria]

Administrative assistants

Aurélie Richard [Sophia, until September 2007]
Dominique Guédon [Sophia, since October 2007]
Françoise De Coninck [Grenoble, until October 2007]
Helen Pouchot [Grenoble, since October 2007]

Technical staff

Bilel Ben Romdhane [Associate Engineer, since November 2007]
Jahanzeb Farooq [Associate Engineer]
Mohamed Amine Chaoui [Expert Engineer, since April 2007]
Lionel Giraud [Associate Engineer, since June 2007]
Mathieu Cunche [Expert Engineer, until March 2007]
Mathieu Lacage [Dream Engineer]
Thierry Parmentelat [Senior Engineer]

Invited Professor

Katia Obraczka [Associate Professor at University of California, Santa Cruz, until July 2007]

Post doc

Anwar Al-Hamra [until August 2007]
Chun-Fai-Aldar Chan [until February 2007]
Thrasyvoulos Spyropoulos [until August 2007]

PhD students

Diego Dujovne [Funding Argentinian Scholarship]
Aurélien Francillon [Funding Ubisec&Sens project, since January 2006]
Mohamed Ali Kaafar [Funding RNRT Oscar, until September 2007]
Mathieu Lacage [INRIA DREAM Engineer]
Mate Soos [Funding INRIA grant]
Naveed Bin Rais [Funding Pakistanian Scholarship, since October 2007]
Mathieu Cunche [Funding ANR contract, since February 2007]
Amine Ismail [Funding CIFRE Scholarship with UDcast, since March 2007]
Mohamad Jaber [Funding MESR Scholarship, since October 2007]
Stevens Le Blond [Funding INRIA CORDIS Scholarship, since September 2007]
Mohamed Karim Sbai [Funding ExpeShare project, since June 2007]

Trainees and Visiting PhD students

Mohamed Karim Sbai [ENSI, Tunis, until February 2007]
Medhi Msakni [ENSI, Tunis, until March 2007]
Amir Krifa [ENSI, Tunis, from February to June 2007 and since September 2007]
Ahmed Ayadi [ENSI, Tunis, from February to June 2007 and since September 2007]
Mounir Chadid [Ecole Polytechnique, France, from April to July 2007]

Pawel Marciniak [Poznan University of Technology, Poland, from March to June 2007]
Federico Maguolo [Univ Padova, Italy, Visiting PhD Student, since November 2007]
Ersin Uzun [University of California, Irvine, Visiting PhD Student, from September to December 2007]

2. Overall Objectives

2.1. Overall Objectives

Keywords: *Heterogeneous networks*, *communication protocols*, *data-centric networking*, *group communication*, *multimedia applications*, *peer-to-peer protocols*, *resource localization*, *security protocols*, *traffic measurement*, *transmission control*.

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 group 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 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).

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 recently started with the COLOR PURPURA project (in collaboration with University of Avignon) and 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

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. 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.

This year, in the context of the OneLab project, and in close collaboration with Princeton University, we have contributed to bring the following enhancements to both the software and the PlanetLab Europe platform:

- Scalability: The PlanetLab public platform has grown up to 800+ nodes and 400+ sites over a four-year period, which is quite a success story. However the current centralized management structure is not likely to scale up to a much more important scale; this is the reason why we have started to run the PlanetLab Europe platform in a **federation** with PlanetLab Central at Princeton. The model, that is totally transparent to users/experimenters, basically allows to aggregate several experimental platforms into a unified one, offering the user the ability to use the whole platform.

  We have been active in designing and implementing this federation paradigm, and plan to go on improving it so as to support a much wider cooperation framework, by breaking the barriers between various experimental testbeds.
- Heterogeneity: On a parallel track, we are planning on studying the impact that a reservation model could have on the current PlanetLab resource allocation scheme. The objectives here are to provide a platform that would be appropriate for both continuous services – and there are quite a few of those that run on PlanetLab on a daily basis – and with experiments that need only a finite amount of time but that, on the other hand, need for various reasons to gain full access to the hardware. This would open the door to much more controlled experimental environments, that are for instance required in the wireless arena.

  This leads at last to the aspects related to virtualization. Although we do not have specific skills in the virtualization techniques per se, we are in a position to take good advantage of the many paradigms and implementation that have become increasingly fashionable recently. We believe that supporting a wider spectrum of these techniques to build the underlying experiment abstraction is likely to widely improve the capabilities of the experimental platform as a whole.

Recall that the evaluation of new network protocols and architectures is at the core of networking research. This evaluation is usually performed using simulations (e.g., NS2), emulations (e.g., Emulab), or in the wild experimental platforms (e.g., PlanetLab). Simulations allow a fast evaluation process, fully controlled scenarios, and reproducibility. However, they lack realism and the accuracy of the models implemented in the simulators is hard to assess. Emulation allows controlled environment and reproducibility, but it also suffers from a lack of realism. Experiments allow more realistic environment and implementations, but they lack reproducibility and ease of use. Therefore, each evaluation technique has strengths and weaknesses. However, there is currently no way to combine them in a scientific experimental workflow. Typical evaluation workflows are split into four steps: topology description and construction, traffic pattern description and injection, trace instrumentation description and configuration, and, analysis based on the result of the trace events and the status of the environment during the experimentation. To achieve the integration of experimental workflows among the various evaluation platforms, the two following requirements must be verified:

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

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

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

To make the use of these components transparent, we plan to implement them within a simulation-like system which should allow experiments to be conducted within a simulator and within the OneLab testbed through the same programming interface. The initial version will be based on the NS3 programming interface.

5. Software

5.1. NS-3 Simulator

NS3 is the followup to the wildly successful NS2 project. NS2 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 NS2 to validate their research. Despite (or because of) this success, NS2 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 NS3 from scratch with NSF funding. Through our involvement in the NS3 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 NS3.

5.2. 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.

5.3. 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.

5.4. 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 are now moving 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. See http://one-lab.org for more details.

5.5. 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/. WisMon will be integrated to OneLab software as a building block toward a global experimental environment.

LCC

LCC (Locate, Cluster and Conquer) is a Two-level clustered overlay multicast architecture that provides scalable, efficient and robust multicast distribution service to end-users. LCC provides a library to handle different useful application-layer functions. However, it is first designed to address topology-aware construction, so focus is set on two major processes : Locating and Clustering. Wrappers for several common MBone conferencing applications have been designed: vic rat, and vlc. LCC is available as open source under the Cecill license, see http://planete.inria.fr/software/LCC/.

TICP

TICP (Transport Information collection Protocol) is a TCP-friendly reliable transport protocol that collects information from a large number of network entities. TICP is a stand-alone protocol that can be used in any application requiring the collection of information: availability of network entities, statistics on hosts and routers, quality of reception in a multicast session, numbering of population, weather monitoring, votes, etc. The source code will be soon released under the Cecill license; for further information see http://planete.inria.fr/chadi/ticp/ .

Intrumentation of BitTorrent

We have instrumented one of the most popular BitTorrent client in order to perform an experimental evaluation of the protocol. This instrumentation allows to log each message sent or received, and internal state of the protocol. This is the first (and only one to the date of this report) complete instrumentation of a BitTorrent client. This is a fundamental step toward the understanding of the dynamics of BitTorrent in reality. The first results obtained with this client were published in IMC'2006, the best international conference on measurements. This instrumented client was publicly released in September 2006 and is available at: http://www-sop.inria.fr/planete/Arnaud.Legout/Projects/p2p_cd.html. To the date of this report this client was downloaded by the community 66 times. This instrumentation was done by Arnaud Legout.

6. New Results

6.1. Data Centric Networking

Participants: Anwar Al-Hamra, Chadi Barakat, Walid Dabbous, Diego Dujovne, Aurelien Francillon, Mohamed Ali Kaafar, Arnaud Legout, Katia Obraczka, Vincent Roca, Karim Sbai, Thierry Turletti, Thrasyvoulos Spyropoulos.

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 2007 in this area.

- **Adding Integrity Verification Capabilities to the LDPC-Staircase Erasure Correction Codes**

  With the advent of broadcast/multicast systems, like DVB-H, 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. FLUTE/ALC). This work focuses on the LDPC-staircase large block FEC codes. We believe that sooner or later these broadcasting systems will require security services. Therefore, the current work focuses on the content integrity service, which is one of the key security building blocks. More and more often (and in particular in the context of DVB-H), the client terminal will be a handheld autonomous device with limited battery capacity. In order to save the client terminal resources, we have focused on a hybrid system that merges the FEC decoding and content integrity verification services. This hybrid system takes advantage of a corruption propagation phenomenon during the FEC decoding process in order to perform integrity verification. Thanks to this approach, we have been able to design a high performance hybrid codec that keeps the same erasure recovery capabilities of the LDPC-staircase codes while providing a Content Integrity Verification service almost for free. More precisely this system can detect an object corruption triggered by deliberate but random attacks or by transmission errors (not detected by lower layer protocols) with a very high probability (close to 100%) with a processing overhead that is only a minimal fraction (around 6%) of the overhead of a hash calculation over the whole object. Finally, we explain how to extend this system in order to provide a 100% detection guarantee, or how this system can help to mitigate a Denial of Service attack.

- **Standardization of FEC Codes for the Erasure Channel within the IETF RMT Working Group**

We are actively participating to the RMT (Reliable Multicast Transport) Working Group of the IETF. In that context, we have continued our efforts on standardizing (presumably IPR-free) FEC codes for the erasure channel, that can be easily plugged within the ALC and NORM transport protocols. More specifically, this activity, initiated in 2005, is now close to the end and the LDPC-staircase/triangle FEC codes proposal as well as the Reed-Solomon FEC codes proposal have both passed working group last call, have been approved by the IESG and entered the RFC Editor waiting queue (Reed-Solomon), or will soon be approved by the IESG (LDPC-*). Note that both documents are meant to be published as "Proposed Standard".

- **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 performed an experimental evaluation of BitTorrent, which is the only one popular peer-to-peer protocol to focus on efficient content delivery. We evaluated its two core mechanisms: its piece selection mechanism called rarest first, and its peer selection algorithm called choke algorithm. We show that the rarest first algorithm guarantees a diversity of the pieces among peers close to the ideal one. In particular, on our experiments, a replacement of the rarest first algorithm with a source or network coding solution cannot be justified. We also show that the choke algorithm in its latest version fosters reciprocation and is robust to free riders. In particular, the choke algorithm is fair and its replacement with a bit level tit-for-tat solution is not appropriate.

  Focusing on the properties of the choke algorithm [16], we showed that it enables clustering of similar-bandwidth peers, ensures effective sharing incentives by rewarding peers who contribute with high download rates, and achieves high upload utilization for the majority of the download duration. We also examined the properties of the new choke algorithm in seed state and the impact of initial seed capacity on the overall BitTorrent system performance. In particular, we showed that an underprovisioned initial seed does not enable clustering of peers and does not guarantee effective sharing incentives. However, we showed that even in such a case, the choke algorithm guarantees an efficient utilization of the available resources by enforcing fast peers to help other peers with their download. Based on our observations, we offered guidelines for content providers regarding seed provisioning, and discussed a tracker protocol extension that addresses an identified limitation of the protocol. This work is the result of a collaboration with Nikitas Liogkas, Eddie Kohler, and Lixia Zhang from UCLA, USA.

- **Disruption Tolerant Networking**

  We start an activity on problems related to efficient routing and buffer management in Disruption (or Delay) Tolerant Networks (DTN). DTNs are networks where a number of traditional assumptions break, and novel communication techniques need to be applied. Two of these techniques that have found considerable success are that of "mobility-assisted routing" and "controlled message replication". We have already identified a family of protocols, called Spray routing, who successfully combine these techniques and achieve close-to-optimal performance in idealized scenarios, where for example all nodes are homogeneous or all nodes are co-operating in forwarding traffic.

  We're currently investigating the performance of these protocols under non-ideal conditions including: losses of message replicas (e.g. queue drops, non-cooperating nodes, etc.), heterogeneous environments, correlated mobility in both time and space. We focus on both evaluating/modeling the performance degradation of these protocols compared with the ideal situation, as well as designing new mechanisms (including history-based algorithms, learning, adaptability) that can overcome these problems and deliver superior performance in diverse conditions.

  In [22], we propose efficient buffer management policies for DTNs. We show that traditional buffer management drop policies like drop-tail or drop-front fail to consider all relevant information in this context and are, thus, sub-optimal. Using the theory of encounter-based message dissemination, we propose an optimal buffer management policy based on global knowledge about the network. Our policy can be tuned either to minimize the average delivery delay or to maximize the average delivery rate. Finally, we introduce a distributed algorithm that uses statistical learning to approximate the required global knowledge of the optimal algorithm, in practice.

Also related to networking in environments subject to episodic connectivity, we have been working on the following activities: (1) Developing a taxonomy for existing mechanisms and protocols, (2) exploring different heuristics for opportunistic message forwarding, and (3) investigating the effects of traffic differentiation on the performance of different routing mechanisms.

- **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 the ExpeShare ITEA European project. 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. It is clear that 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 be very likely propagate in a unique direction from the seed to distant peers. This could prohibit peers from reciprocating data and might lead to 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. Preliminary results on our research in this direction can be found in [29].

- **Securing Network Coordinate Systems**

  We also worked on securing distributing protocols that aim at calculating machines' coordinates [15]. Those protocols are an efficient solution to infer network topology in a distributed way. Their major problem is that they are very sensitive to attacks and malicious behavior. For example, a protocol like Vivaldi and NPS leverages communication and delay measurements between machines to calculate coordinates. If a machine lies on its coordinates or delays packets so that the delay measurement is wrong, this will cause a shift in the coordinates of the other machines. Clearly, the damage is proportional to the number of machines participating to the attack. A shift in the coordinates of the attacked machines results in a degradation in the performance of any application using these coordinates like file sharing and content distribution. At the same time, the attacking machines can profit from this shift to improve their performances. To solve the problem, we came up in [15] with an elegant solution in which delay prediction with reliable machines is tracked by a Kalman filter. By doing like this, when a malicious machine lies on its coordinates or delay measurement, there will be a deviation in the prediction from the expected value calculated by the Kalman filter, which allows its detection. To calibrate the Kalman filter on reliable machines, we proposed the deployment of a surveyor infrastructure composed of reliable machines, then we use the Kalman filter calibrated at one surveyor at neighboring non surveyor machines. We proved by the means of simulations and real experiments that by using our solution, coordinate systems can resist to attacks and eliminate them. Our work continues in this direction with the proposition of a time validity period every time the surveyor gives its Kalman filter parameters to neighboring machines. Indeed, due to changes in network conditions, these parameters can change with time and so it is very important that nodes that use them stop doing it and seek for new parameters.

6.2. Security in infrastructure-less and constrained networks

Participants: Claude Castelluccia, Chun-Fai-Aldar Chan, Aurelien Francillon, Mate Soos, Erzin Uzun.

- **TinyRNG**

  WSN security is a major concern and many new protocols are being designed. Most of these protocols rely on cryptography, and therefore require a cryptographic pseudo-random number generator (CPRNG). However designing an efficient and secure CPRNG for wireless sensor networks is not trivial since most of the current source of randomness used by standard CPRNG are not present on a wireless sensor node. We have developped TinyRNG, a CPRNG for wireless sensor nodes. Our generator uses the received bit errors as one of the sources of randomness. We showed that transmission bit errors on a wireless sensor network are a very good source of randomness. We demonstrated that these errors are randomly distributed and uncorrelated from one sensor to another. Furthermore we showed that these errors are difficult to observe and manipulate by an attacker. This work was presented at the WiOpt'07 conference [14].

- **Private Aggregation and Group Communication in Wireless Sensor Networks**

  Wireless sensor networks (WSNs) are ad-hoc networks composed of tiny devices with limited computation and energy capacities. For such devices, data transmission is a very energy-consuming operation. It thus becomes essential to the lifetime of a WSN to minimize the number of bits sent by each device. One well-known approach is to aggregate sensor data (e.g., by adding) along the path from sensors to the sink. Aggregation becomes especially challenging if end-to-end privacy between sensors and the sink is required.

  We developped in the last years a simple additively homomorphic stream cipher that allows efficient aggregation of encrypted data. The new cipher only uses modular additions (with very small moduli) and is therefore very well suited for CPU-constrained devices.

  In 2007, we have worked on a formal treatment to the privacy of concealed data aggregation (CDA). While there exist a handful of constructions, rigorous security models and analyses for CDA are still lacking. We have refine standard security notions for public key encryption schemes, including semantic security and indistinguishability against chosen ciphertext attacks, to cover the multi-sender nature and aggregation functionality of CDA in the security model. We have also proposed a generic CDA construction based on public key homomorphic encryption, along with a proof of its security in the proposed model. The security of two existing schemes was analyzed in the proposed model. This work was presented at Esorics 2007 [12].

  We have also developped, this year, a new encryption mode of operation of our previously defined homomorphic stream cipher that allows nodes of a network to exchange messages securely (i.e. encrypted and authenticated) without sharing a common key or using public key cryptography. Our scheme is well adapted to networks, such as ad hoc, overlay or sensor networks, where nodes have limited capabilities and can share only a small number of symmetric keys. It provides privacy and integrity protection. We show that our proposal can be used in wireless sensor networks to send encrypted packets to very dynamic sets of nodes without having to establish and maintain group keys. These sets of nodes can be explicitly specified by the source or can be specified by the network according to some criteria, such as their location, proximity to an object, temperature range. As a result, a node can, for example, send encrypted data to all the nodes within a given geographical area, without having to identify the destination nodes in advance. Finally we show that our proposal can be used to implement a secure and scalable aggregation scheme for wireless sensor networks This work was presented at the IEEE MASS conference [9].

- **Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks**

  Wireless sensor networks are usually deployed to operate for a long period of time. Because nodes are battery-operated, they eventually run out of power and new nodes need to be periodically deployed to assure network connectivity. This type of networks is referred to as Multi-phase WSN.

Existing schemes are not adapted to multi-stage WSN. With these schemes, the security of the WSN degrades with time, since the proportion of corrupted links gradually increases. We proposed a new pre-distribution scheme adapted to multi-phase WSN. In the proposed scheme, the pre-distributed keys have limited lifetimes and are refreshed periodically. As a result, a network that is temporarily attacked (i.e. the attacker is active only during a limited amount of time) automatically self-heals, i.e. recovers its initial state when the attack stops. In contrast, with existing schemes, an attacker that corrupts a certain amount of nodes compromises a given fraction of the total number of secure channels. This ratio remains constant until the end of the network, even if the attacker stops its action. Furthermore, with our scheme, a network that is constantly attacked (i.e. the attacker regularly corrupts nodes of the network, without stopping) is much less impacted than a network that uses existing key pre-distribution protocols. With these schemes, the number of compromised links constantly increases until all the links are compromised. With our proposal, the proportion of compromised links is limited and constant. This work was presented at the SecureComm07 conference [11].

- **RFID Security/Secret Shuffling** In this project, we consider the problem of private identification of very small and inexpensive tags that cannot perform any cryptographic operations. We have developped a new scheme (ProbIP) that does not require any computation from the tag. Our scheme resembles Juels' pseudonym-rotation scheme, but increases its security significantly. The presented scheme is an identification scheme. As such, it does not address authentication, and so can not be used to authenticate a tag. It serves to correctly identify a tag if no active attacker is present. Privacy of the tag is preserved to some extent even if an active attacker is present. The proposed scheme relies on an NP-complete problem and as such is proven to be difficult to breach. This work was presented at the RFIDSEC'07 conference [10].
- **Spam detection** We worked on the problem of botnets and spams detections in collaboration with Ersin Uzun, UCI Phd candidate, invited in the context of the UbiSec associated team with UC Irvine. We've developped the concept of "proof of presence" that authorized the emission of emails only if the sender server is convinced that the user is sitting behind its computer.

6.3. Network monitoring

Participants: Chadi Barakat, Arnaud Legout, Karim Sbai.

The main objective of our work in this domain is a better monitoring of the Internet and a better control of its resources. In the monitoring part, we work on new measurement techniques that scale with the fast increase in Internet traffic and growth of its size. 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. In particular, we propose efficient drop and routing mechanisms for Disruption Tolerant Networks, as well as analytical models that allow a better understanding of the performances of network protocols.

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

- **A Multilevel Approach for the Modelling of Large TCP/IP Networks** We worked on an analytical model for the calculation of network load and drop probabilities in a TCP/IP network with general topology. Our model does not require the predefinition of bottleneck links. The model is based on analytical expressions for TCP throughput, which allows it to take into account diverse TCP features as the receiver congestion window limitation. It can be used for TCP/IP networks with drop tail routers as well as for TCP/IP networks with active queue management routers. First, we formulate our model as a Non- Linear Complementarity problem (NCP). Then, we transform the model into two equivalent formulations: fixed point formulation and nonlinear programming formulation. Thereupon, using asymptotic analysis, we prove existence of a unique solution to the NCP by casting it into the well known utility optimization framework. In addition to uniqueness of rates and end-to-end drop probabilities, the NCP shows the ability to provide unique solutions in terms of link drop probabilities. We explain the relationship between the utility optimization, fixed-point approach and our complementarity approach. Specifically, we show how these models can be derived from each other. Finally, we illustrate the utility of our proposed approach by solving some benchmark examples and showing how the distribution of load varies with network parameters. The distribution of load is sometimes counter-intuitive which cannot be detected by other models making prior assumptions on the locations of bottlenecks. This work was presented at the final meeting of the COST 285 project and appeared as a Chapter in [2].

- **Inter-protocol fairness between TCP New Reno and TCP Westwood+**

  This work started with the visit of Niels Moller (PhD student at KTH) to Planète and was done in collaboration with the Maestro group. In this work, we investigate the effect of introducing TCP Westwood+ on regular TCP New Reno. By means of analytical modeling and ns-2 simulations, we demonstrate that the two protocols get different shares of the available bandwidth in the network. Our main result is that the bandwidth sharing between the two protocols depends on one crucial parameter: the ratio between the bottleneck router buffer size and the bandwidth delay product. If the ratio is smaller than one, TCP Westwood+ takes more bandwidth. On the contrary, if the ratio is greater than one, it is TCP New Reno which gets the larger part. Inspired by our results, we propose a simple modification to the window decrease algorithm in TCP Westwood+ that solves the unfairness problem for large buffer sizes. For small buffers, the unfairness problem is still open. Our results were published in [17].

- **TICP: Transport Information Collection Protocol**

  We keep improving and validating TICP, our TCP-friendly reliable transport protocol to collect information from a large number of Internet entities. A collector machine sends probes to a set of information sources that reply by sending back their reports. TICP adapts the sending rate of probes in a way similar to TCP for the purpose of avoiding network congestion and implosion at the collector. Lost reports are requested again by TICP until they are correctly received by the collector. In a first part of this work, we add to TICP a mechanism to cluster information sources in order to probe sources behind the same bottleneck together. This ensures a smooth variation of network conditions during the collection session and hence, an efficient handling of congestion at network bottlenecks. We run simulations in ns-2 over realistic topologies to compare TICP before and after clustering. We also implement the protocol in C++ and test it over the PlanetLab platform. All experiments prove the outperformance of TICP over non adaptive solutions and the interest of the clustering mechanism in shortening the duration of the collection session and in decreasing the ratio of lost packets. In a second part, we adapt TICP to collect large amounts of information from each data source. By the means of simulations, we compare the performance obtained by TICP to that obtained when the information maintained by the different sources is collected by parallel TCP connections. Again, the simulations show that TICP yields shorter collection sessions due to its inherent multiplexing capability. Finally, in a last part, we study the impact of delegating collection to some proxy sources that collect from other sources on behalf of the collector and that the collector probes later to get their collected data. We explain our method to choose the proxy collectors and we show by simulations that for a judicious choice of proxy collectors, one can decrease considerably the collection session duration. All details can be found in [28].

- **Chaotic behavior in computer networks**

  Chaos is a prominent feature of complex systems and dynamical systems theory provides methods for analyzing this kind of behavior. Computer networks are complex systems, but it is not yet known whether Internet protocols exhibit chaotic behaviors though some preliminary investigations suggest it. Understanding the meaning and effect of such behaviors is a scientific challenge, with the potential of a significant impact, especially concerning applications based, e.g., on chaos control, or resonances in chaotic systems. For this, on the one hand, one needs to design models describing properly the dynamic evolution of a computer network using an Internet protocol, and to make the mathematical analysis of these models. On the other hand, one must perform careful investigations on real protocol traces, to analyze them with the tools developed in chaos theory, and to compare them to the predictions of the models. We have performed extensive simulations of TCP on deterministic scenarios and have observed a complex dynamics even in simple scenarios. We are analyzing our results to understand the reason of this dynamics. This work is in collaboration with Bruno Cessac from the INLN, Sophia Antipolis, France.

- **Network Measurments Processing Tool**

  WisMon is a complete network (wireless+wired) experimentation package which consists in the implementation of a measurement, processing and analysis methodology. Current development is oriented towards the definition of an experiment-description protocol, an experiment scheduling engine, and the definition of the data structure for database storage. Further work includes the capture log preprocessing module, the data post-processing and analysis module to generate results based in queries on the preexistant database.

6.4. Network Evaluation Platforms

Participants: Walid Dabbous, Jahanzeb Farooq, Mathieu Lacage, Thierry Parmentelat, Thierry Turletti.

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 the OneLab project, 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.

- **Federating Research Testbeds**

  In cooperation with Princeton University who run the PlanetLab research platform, we have developped the first prototype of a federation paradigm, 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.

We plan on keeping improving this functionality. Scalability is not an immediate concern yet as there are at this time no deployed testbed with more than 3 peers. However there are clear indications that this could very well become a heavy trend in the future, as it is for instance the paradigm behind the GENI initiative. Our next challenges will be to define a hierarchical namespace for all involved objects in the system - a la DNS - and to take advantage of that tree structure to break the currently n-square peering model into an essentially linear one. Policy management will also be improved once PlnetLab Europe has gained sufficient feedback on the actual needs in this area.

- **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 to be natively integrated in the 4.2 release of the PlanetLab software, that is about to be issued.

- **Enhancing network simulations**

  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 approach focuses on two solutions:

  - allow users to run unmodified (or very lightly modified) real-world code in the network simulator at the application and networks layers
  - implement detailed MAC and PHY models of common wireless technologies such as 802.11 and Wimax.

  To evaluate this line of research, we have developed a simulator, named YANS. This initial prototype showed the feasability of the approach and we have merged our effort with the ns-3 project, contributing therefore to the development of the ns-3 architecture. Since then, we have been associated to the development of the core infrastructure of the ns-3 simulator: we contributed the event scheduler and the packet data structure used in ns-3. We also contributed to the specification and refinement of the core ns-3 Node data structure. In the future, we plan to keep contributing to architectural discussions and we hope to influence the associated decisions to allow us to realize our vision of a simulator used as a more controllable real-world testbed.

  As for the development of MAC/PHY models, we started two years ago: we developed a 802.11a/e MAC and PHY model in ns-2. This model implementation was subsequently ported to the YANS simulator to validate its architecture and has been ported and integrated to ns-3 in december 2007. We also worked on rate control algorithms support. Federico Maguolo is focusing on improving the validation methodology of these algorithms. His objective is to use a set of well-defined reference simulation scenarios to perform a comprehensive study of existing rate control algorithms with an eye towards the design and implementation of a rate control algorithm which can work efficiently in a wide variety of use-cases.

Last year, we started developing a Wimax MAC model for ns-3. This effort is continuing this year currently focused on the identification of the components required in our model. i.e., we cannot afford to implement all of the specification given our manpower so, we need to identify the relevant components required to perform the type of application-level simulation we are interested in. We have started the development work by realizing a simplified PHY layer. This PHY simply transmitted bursts received by the MAC layer, ignoring the underlying PHY layer details. Next the work started on the development of the MAC layer. Some of the primary functionalities of the WiMAX MAC layer, both for the SS (Subscriber Station) and the BS (Base Station) side, were implemented. The functionality of generating downlink/uplink subframes and transmitting MAC control messages (DL-MAP, UL-MAP, DCD, UCD, etc) was implemented at the BS. MAC control messages are an essential part of the MAC layer since they are used to allocate the stations the access to the downlink and uplink channels. Furthermore it included the functionality of allocating bursts in UL/DL subframes and the construction and transmission of PDUs in these bursts. At the SS side the functionality to read the subframes and the MAC control messages was implemented. The MAC implementation also includes the network entry and initialization functionality, the process which a SS follows while entering into a WiMAX network. It includes scanning of the frequency channels, exchange of handshake messages (Ranging messages) containing the necessary parameters defining the network, and adjustment of these parameters etc. Meanwhile a new, complete WiMAX OFDM PHY implementation developed at UP6 was made available to be integrated with the MAC layer. Since this PHY layer operated on bits streams, a complete interface API was written to integrate it with the MAC layer. With this interface the bursts transmitted at the MAC layer are splitted into smaller blocks, converted into bit streams and then transmitted on the wireless medium. With this new OFDM PHY layer implemented, the MAC layer can now be used with either of the two PHY layers.

7. Other Grants and Activities

7.1. National projects

- RNRT Oscar (2006-2007): The Planète project-team is involved in the OSCAR RNRT project which aims at studying the attacks against P2P overlays and their impact on the underlying network infrastructure. This work is going in three parts: (1) in the first part, we perform an extensive study of the state-of-the-art on attacks in P2P networks and more precisely in BitTorrent; (2) In the second part, we are studying a new attack, namely the Sybil attack, which was already proposed in the context of improving the performances of cheaters and not in the context of attacking the overlay. The basic idea of such an attack is to breakdown the torrent by introducing free riders. First of all, free riders will occupy partially the available upload capacity at the seeds. Moreover, when having many free riders as neighbors, a node will have fewer sources for the pieces it needs and consequently, it will spend more time to download the file; (3) In the third part, we are showing the danger that BitTorrent can present on the network infrastructure. We want to evaluate how the BitTorrent traffic can be redirected in such a way to increase significantly the load on some specific links and by how much this can harm the underling network.

  The project involves teams from both academy and industry, such as LAAS, LIP6, France Telecom, Mitsubishi, ENS Lyon and ENST Bretagne.

- The Sesur RFID-AP project is a ANR project that has started end of 2007 for 3 years. The project partners are CEA-LETI, France Télécom R&D, Eurecom and INRIA.

  The widespread deployment of RFID tags is gathering pace around the world. These tags reply to the electronic prompts of a reader and can be used to store unique product identifiers such as the make and style of a piece of clothing or a unique identifier for a bottle of pharmaceutical. At the same time, however, it is well-known that such tags and their applications are not without risk. There are many security issues associated with the use of such devices ranging from the prevention of tag-cloning through to issues such as respecting the privacy rights of individuals.

The purpose of the RFID-AP project is to consider the range of security threats to applications based on the deployment of RFID-tags and to concentrate on two particular issues; those of authentication and privacy. While these are often presented as two different issues, many of the precautions we might take to protect our privacy are based on taking appropriate steps for authentication, for instance in ensuring that we only reveal tag information to a legitimate, i.e. authenticated, reader.

The goal of RFID-AP, therefore, is to design and to prototype cryptographic algorithms and secure protocols for RFID deployment. Such algorithms and protocols could be used individually, or in combination, and our hope is that these will provide a practical and useful framework within which to apply innovative but practical techniques for device authentication and user privacy.

- RNRT CAPRI-FEC (2007-2009): this project focuses on a building block that is critical to many networking applications: FEC for the packet erasure channel. These codes, that usually operate at the transport or Application Layer (hence their name, AL-FEC), are complementary to FEC working at the physical layer. One benefit is that AL-FEC are easily implemented in software codecs, which provides a lot of flexibility: they can operate on very large blocks, whereas physical layer codes are often limited by the available chipset memory, they can integrate the application constraints by dynamically varying the size of the encoded blocks, the amount of redundancy added, or even by providing several levels of protection. This project aims at analyzing and comparing various AL-FEC, both from a theoretical point of view and in practical applications, to derive the conditions for their optimal use.

  Partners: INRIA Planète project-team (leader), ENSICA, CEA-LETI, STMicroelectronics, and a company that wants to remain anonymous.
- ANR CIS Hipcal (2007-2009): this project studies a new paradigm based on confined virtual cluster concept for resource control in grids. In particular, we study and implement new approaches for bandwidth sharing and end to end network quality of service guarantees. The global infrastructure (computers, disks, networks) partitioned in virtual infrastructures (aggregation of virtual machines coupled with virtual channels) is dynamically composed. These virtual clusters are multiplexed in time and space, isolated and protected.

  Partners: INRIA Reso (leader), INRIA Grand Large, INRIA Planète, I3S Nice University, IBCP.
- ANR Divine project (2006-2008): The DIVINE ANR project proposes the study and the development of a simple yet realistic system of video and image transmission towards heterogeneous mobile terminals (for instance PDA or digital TV receiver) through heterogeneous wireless and wired IP links. The application aimed by the DIVINE project is the interactive access to multimedia data in a museum. This is a typical environment where various techniques of wireless (WLAN, WiMAX) and wired transmission can be jointly exploited. The DIVINE project aims to study innovative solutions (scalable video and still image coding, unequal error protection, multicast links, multiple description coding) allowing to perform an end-to-end optimization, based on the detection, optimal management and adaptive processing of this heterogeneity. The project has started in July 2006 and involves teams from both industry and academy as Thales, France Télécom R&D, ETIS, ENST Paris, L2S, LIP6 and the research center of French Museums C2RMF-UMR171. At Planète, we focus in particular on the design and the evaluation of multicast multimedia transmission mechanism for IEEE 802.11 WLANs.
- CPER Plexus: This project (2007-2010) 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.

7.2. European projects

- OneLab: The OneLab project (2006-2008) has two overarching objectives: (1) To extend the current PlanetLab infrastructure. OneLab widens PlanetLab by adding testbed nodes behind links that are not typical research network links. OneLab will also deepen PlanetLab by enhancing the ability of applications that are running on PlanetLab to perceive the underlying network environment: viewing the packets that pass through certain points in the network, and viewing the topology of the network. (2) To create an autonomous PlanetLab Europe. OneLab takes over the administration of PlanetLab nodes across Europe, and enters into a peering relationship with PlanetLab in the United States.

  OneLab introduces several new components to the PlanetLab testbed: Wireless (WiMAX, UMTS, and ad hoc wireless), Wired (multihomed), An emulation component and Monitoring (passive monitoring, and topology information components).

  The project partners are UPMC, INRIA, Intel (until December 06), UC3M, UCL, CINI, FT, UniPi, Alcatel Italia and TP. INRIA is strongly invlolved in the project and has the role of technical leader.

- Expeshare (2007-2009) 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 will be 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 will study the feasibility of running actual Peer-to-Peer solutions over wireless networks and try to understand their limitations and based on that, propose new solutions to efficiently localize resources in a wireless network and share it with other interested users. The propositions made by INRIA will be the subject of integration to modules proposed by other partners and evaluation over by simulation and real experimentations.

  Planète works in this project jointly with the Hipercom project-team known by its expertise in the domain of routing in ad hoc networks. Namely, one of the key questions in Expeshare is how to make an ad hoc routing protocol like OLSR, the routing protocol developed by HIPERCOM, interacts with a P2P architecture for data sharing. The expertise of Hipercom in the routing domain and of Planète in the P2P domain are of major importance to INRIA's contribution in the project. The project started in April 2007 and will last until June 2009.

- The UbiSec&Sens project is an European funded project under the FP6 "Trust and Security" program. It has started in 2006 for a period of 3 years. Its partners are EURESCOM , RWTH Aachen, INRIA, IHP Microelectronics, INESC/INOV, Budapest University of Technology and Economics, Ruhr University Bochum and NEC Europe Ltd.

  The overall objective of UbiSec&Sens is to develop a comprehensive architecture for medium and large scale wireless sensor networks with the full level of security that will make them trusted and secure for wide-scale applications. The project focuses its work on the intersection of security, routing and in-network processing to design and develop efficient and effective security solutions and to offer effective means for persistent and encrypted data storage for distributed (and tiny) data base approaches. It will provides a complete toolbox of security aware components for sensor network application development. The UbiSec&Sens solutions will be prototyped and validated in the representative wireless sensor application scenarios of agriculture, road services and homeland security.

7.3. 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.

Genesim: (2007-2010) is an associated team between University of Washington (Prof. S. Roy) and INRIA Planète project-team. Evaluation of new network protocols and architectures is at the core of networking research. This evaluation is usually performed using simulations, emulations, or experimental platforms. Each of these evaluation techniques has strengths and weaknesses and therefore they complement one another. However, there is currently no way to combine them in a scientific experimental workflow. On the other hand, wireless network protocols are challenging to evaluate mainly due to the high variability of the channel characteristics and their sensitivity to interference. Indeed, as the wireless environment is very difficult to control, repeatable experiments are complex to perform. In addition, a large number of parameters impact the results of an experiment. It is therefore difficult to find the subset of key parameters to be taken into account to characterise a wireless experiment. The objective of this Associated Team is to contribute toward this area by providing a prototype evaluation environment for wireless experiments.

This evaluation environment is based on a common programming interface between ns-3, Orbit and OneLab. This prototype will allow running basic wireless networking scenarios on these three environments and to compare the simulations and experiments' results. Based on University of Washington competence on Orbit and ns-3 and on INRIA's competence on OneLab and ns-3 we expect this common project to have a high impact on both European and International consortiums.

Color PURPURA (2007): This project addresses the problem of peer-to-peer data exchange in an ad hoc network in an efficient way. We will focus in particular on the content replication taking into account the network constraints (resources scarcity, interference, mobility, medium sharing, etc.) The partners are: Planète and LIA (Laboratoire d'Informatique d'Avignon).

Wireless Networks (STIC Tunisia): This project (2007-2008) aims to address the problems of security and quality of service routing in Wireless Mesh Networks and of reliability in Delay Tolerant Networks. The project partners are ENSI (Tunisia), Eurecom. Several visits have taken place in the context of this project in 2007: Sonia Mettali Gammar and Lamia Ben Azzouz from ENSI visited the Planète project-team for one week in July 2007. Mohamed El-Hdhili from ENSI visited Planète from November 28th to December 19th 2007. Amine Elabibi from ENSI visited Planète from December 12th to December 21st 2007.

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.

8. Dissemination

8.1. Promotion of the Scientific Community

Walid Dabbous has served in the following conferences as PC member : Med-hoc-net' 2003, NGC'(99-2003), SAINT'2001, Networking'2000, ISCC'2000, AFRICOM'98, ICCC'97, PC co-chair of PfHSN'96, tutorial chair for Sigcomm'97, WOSBIS (97-99), CFIP (97-05), CoNext'05, INFOCOM'06, GC'08 CCNS. He gave several presentations and tutorials at RHDM summer school, CFIP, HPN, FORTE and ECMAST. 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 responsible of the University of Nice Sophia Antipolis Master program on Networking and Distributed Systems. He was co-chair of the udlr working group at the IETF between 1997 and 2000. He has served several times as an expert to the European Commission to evaluate and review EC funded projects. He has also served as an expert in RNRT commission on network protocols and architecture. He gave a presentation at the"Université de tous les savoirs" in September 2000. He also gives seminars at the technical and scientific high military education society.

Claude Castelluccia is the editor of the area"Protocols for Mobility" of the ACM SIGMOBILE Mobile Computing and Communications Review (MC2R). He has served in the following conferences as PC member : IPCN2000 (Paris), ACM WoWMoW 2000 (Boston), Globecom2000 Service Portability Workshop (San Francisco), IPCN2001 (Paris), IEEE Services & Applications in the Wireless Public Infrastructure (Paris), MS3G2001 (Lyon), IEEE LCN2001 (Orlando), MobileADHOC networks (Paris), IFIP Networking 2002 (Pisa), IEEE LCN2002 (Orlando), Algotel2002, ACM/Usenix Mobisys 2003 (San Francisco), IEEE LCN2003 (Munich), IEEE Workshop on Applications and Services in Wireless Networks 2003 (Berne). Claude Castelluccia is co-organizer of ESAS (European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks) and is in the PC of several security conferences such as SecureComm'05, Madness'05, TSPUC'05. He has served several times as an expert to the European Commission to evaluate and review EC funded projects.

Thierry Turletti is in the Program Committee of the following conferences/workshops: BroadWiM'04, Packet Video'99-07, Saint'00, Networked Group Communication (NGC)'02, Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)'03-05, Next Generation Networks (NGN)'04, the 2nd International Workshop on Wireless Network Measurement (WinMee'06) and the IEEE International Symposiums on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'05-07). He was chair of the ACM Multimedia Doctoral Symposium in December 2002. He coedited two special issues on software radios in IEEE JSAC and IEEE Communication Magazine in 1999. Since 2001, he is associated editor of the *Wireless Communications, Mobile Computing* 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. Thierry Turletti has served several times as an expert to the European Commission to evaluate and review EC funded projects and also to review French ANR funded projects.

Chadi Barakat was guest editor for a JSAC special issue on Sampling the Internet: Techniques and Applications, PC co-chair for the ResCom 2007 summer school on the future Internet and Autonomous Networks, PC co-chair for the SAMPLING 2005 workshop, general chair for WiOpt 2005 workshops, and general chair for PAM 2004. Currently he is area editor for ACM Computer Communication Review (2005 -) and steering committee member for PAM conference (Passive and Active Measurement). He served (is serving) on the technical Program Committee for WinMee 2008, PFLDnet 2008, BroadNets 2008, NSTools 2007, SECON 2007, WWIC 2007, IWQoS 2006, WWIC 2006, WONS 2006, WiNMee 2006, IMC 2005, ICNP 2005, PAM 2005, WONS 2005, INFOCOM 2005, ASWN 2004, GI& NGN symposium at Globecom 2004, PAM 2004, INFOCOM 2004, ASIAN 2002, ICNP 2002. Chadi Barakat was invited to give talks at COST 285 final symposium (Surrey, UK) 2007, Asian school (Bangkok) - 2005, E-next school (Louvain) - 2005, KTH (Stockholm) - 2005, ENSI (Tunis) 2003 ...2007, MIT (Boston) - 2004, UMASS (Amherst) - 2004, Boston University (Boston) - 2004, Intel Research Cambridge - 2004, Asian school (Bangkok) - 2003, Ecole Normale Supérieure (Paris) - 2003, Ecole d'été Internet Nouvelle Génération (Porquerolles) - 2003, EPFL Summer Research Institute (Lausanne) - 2002, IBM (Zurich) - 2001. Chadi Barakat is member of the recruitment committee at the computer science department of the University of Nice-Sophia Antipolis, member of the directorial board for the Master RSD of the University of Nice, and responsible of the internship program at the latter Master.

Vincent Roca was the main technical organizer of the RHDM'02 summer school, in May 2002. He organized the next International Workshop on Multimedia Interactive Protocols and Systems (MIPS) in Grenoble in 2004. He gave several tutorials in the RHDM summer schools, at ICT'03 and at MIPS'03. He is 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 has served as a PC member of SIGCOMM'2007 (PC heavy), SIGCOMM'2006 (PC light), SIGCOMM'2005 (Shadow PC). 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). Finally he is the organizer of the Planète Ph.D. students seminar (2005).

8.2. University Teaching

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

Networks: Course at Networks and Distributed Systems graduate studies program at University of Nice-Sophia Antipolis, by W. Dabbous (24h).

Internet Measurements: Optional course at Networks and Distributed Systems graduate studies program at University of Nice-Sophia Antipolis, by C. Barakat (18h).

Internet Measurements: Same course given for the students of the Computer Sciences Master at ENSI, the Tunisian National School on Computer Sciences, Tunisia, by C. Barakat (18h).

Introduction to Networking: Undergraduate course at IUT Nice - LPSIL class, by C. Barakat (15h).

Local Area Networks : Undergraduate course + practical work at IUT Sophia-Antipolis, by C. Barakat (25h).

Internet Topolgy inference: Graduate Course at Master RTM of the IUP Avignon, by C. Barakat (7h).

Wireless Communications: Undergraduate course at Polytech' Grenoble, on Wireless Communications, by V. Roca (6h).

Wireless Communications: Same course given to the students of Master 2, GI, University Joseph Fourier, Grenoble, by V. Roca (6h).

Mobile Networks: Course at graduate studies program at Ensimag, by C. Castelluccia (36h).

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

Programming: Course IUT GTR 2005 (36h), by Arnaud Legout

Programming: Course IUT GTR 2006 (30h), by Arnaud Legout

Networks: Course IUT GTR 2006 (30h), by Arnaud Legout

Peer-to-peer networks: Course master RSD at University of Nice-Sophia Antipolis 2006 (15h), by Arnaud Legout

Programming: Course IUT GTR 2007 (30h), by Arnaud Legout

Peer-to-peer networks: Course master RSD at University of Nice-Sophia Antipolis 2007 (15h), by Arnaud Legout

8.3. PhD Theses and Internships

8.3.1. PhD defended in 2007

1. Mohamed Ali Kaafar has defended his PhD in September 2007. He studied the security of Internet coordinate systems [1].

8.3.2. Ongoing PhDs

1. Diego Dujovne works on “Wireless Experimental Test-beds”.
2. Mathieu Lacage works on “An IP-level network topology and link characteristic measurement tool”.
3. Aurélien Francillon works on “WSN security”.
4. Mate Soos works on“RFID Security”.
5. Naveed Bin Rais works on “Adaptive Communication Mechanisms for Networks with Episodic Connectivity”.
6. Mathieu Cunche works on “Forward Error correction codes for the erasure channel ”.
7. Amine Ismail works on “Optimisation of IP Protocols and Applications over Broadcast Links”.
8. Mohamad Jaber works on “Detection and Troubleshooting of Internet Anomalies”.
9. Stevens Le Blond works on “Next Generation Peer-to-Peer Infrastructures”.
10. Mohamed Karim Sbai works on “Architecture for data sharing in wireless network"”.

8.3.3. Training activities

1. Mohamed Karim Sbai,
   Subject: Large Scale Data Collection,
   Supervisor: Chadi Barakat,
   Duration of the stay: 6 months,
   Prepared degree: Master in Computer Sciences,
   Affiliation: ENSI Tunisia.
2. Medhi Msakni,
   Subject: Multicast Support in 802.11 Networks,
   Supervisor: Thierry Turletti,
   Duration of the stay: 7 months,
   Prepared degree: Master in Computer Sciences,
   Affiliation: ENSI Tunisia.
3. Amir Krifa,
   Subject: Buffer Management in DTNs,
   Supervisors: Thierry Turletti and Chadi Barakat
   Duration of the stay: 9 months,
   Prepared degree: Master in Computer Sciences,
   Affiliation: ENSI Tunisia.
4. Ahmed Ayadi,
   Subject: Scalable video transmission in heterogeneous environments,
   Supervisor: Thierry Turletti,
   Duration of the stay: 9 months,
   Prepared degree: Master in Computer Sciences,
   Affiliation: ENSI Tunisia.
5. Mounir Chadid,
   Subject: Implementation of a BitTorrent tracker extension,
   Supervisor: Arnaud Legout,
   Duration of the stay: 3 months,
   Prepared degree: Engineering Degree in Computer Sciences,
   Affiliation: Ecole Polytechnique.

6. Pawel Marciniak,
   Subject: Impact of piece size on peer to peer replication,
   Supervisor: Arnaud Legout,
   Duration of the stay: 4 months,
   Prepared degree: Master in Computer Sciences,
   Affiliation: Poznan University of Technology.

9. Bibliography

Year Publications

Doctoral dissertations and Habilitation theses

[1] M. A. KAAFAR. *Securing Internet Coordinates Systems*, PhD thesis, Université de Nice Sophia Antipolis, September 2007.

Articles in refereed journals and book chapters

[2] E. ALTMAN, K. AVRACHENKOV, C. BARAKAT, K. CHANDRAYANA. *A Multilevel Approach for the Modelling of Large TCP/IP Networks*, in "Recent Advances in Modeling and Simulation Tools for Communication Networks and Services", A. N. INCE, A. BRAGG (editors), Springer US, September 2007.

[3] C. CASTELLUCCIA, N. SAXENA, J. YI. *Robust Self-Keying Mobile Ad Hoc Networks*, in "Computer Networks", vol. 51, n^o 4, 2007.

[4] W. DABBOUS, T. TURLETTI. *Scalable Virtual Environments*, in "Multimedia Multicast on the Internet", A. BENSLIMANE (editor), ISTE, January 2007.

[5] V. ROCA. *End to end approaches for reliable communications*, in "Multimedia Multicast on the Internet", ISTE, January 2007.

[6] V. ROCA. *Reliability in group communications: an introduction*, in "Multimedia Multicast on the Internet", ISTE, January 2007.

[7] J. VILLALÓN, P. CUENCA, L. OROZCO-BARBOSA, Y. SEOK, T. TURLETTI. *ARSM: A Cross-Layer Auto Rate Selection Multicast Mechanism for Multi-Rate Wireless LANs*, in "IET Communications, Special Issue on Wireless Mobile Networks: Cross-layer Communication", 2007.

[8] J. VILLALÓN, P. CUENCA, L. OROZCO-BARBOSA, Y. SEOK, T. TURLETTI. *Cross-Layer Architecture for Adaptive Video Multicast Streaming over Multi-Rate Wireless LANs*, in "IEEE JSAC Special Issue on Cross-Layer Optimized Wireless Multimedia Communications", vol. 25, n^o 4, May 2007, p. 699-711.

Publications in Conferences and Workshops

[9] C. CASTELLUCCIA. *Securing Very Dynamic Groups and Data Aggregation in Wireless Sensor Networks*, in "IEEE International Conference on Mobile Ad-hoc and Sensor Networks (MASS 2007), Pisa, Italy", October 2007.

[10] C. CASTELLUCCIA, M. SOOS. *Secret Shuffling: A Novel Approach to RFID Private Identification*, in "Conference on RFID Security (RFIDSec07), Malaga, Spain", July 2007.

[11] C. CASTELLUCCIA, A. SPOGNARDI. *RoK: A Robust Key Pre-distribution Protocol for Multi-Stage Wireless Sensor Networks*, in "IEEE Securecomm, Nice, France", September 2007.

[12] A. CHAN, C. CASTELLUCCIA. *On the Security of Concealed Data Aggregation*, in "European Symposium On Research in Computer Security (ESORICS 2007), Dresden, Germany", September 2007.

[13] D. DUJOVNE, T. TURLETTI, W. DABBOUS. *Experimental Methodology for Real Overlays*, in "2nd International Workshop on Real Overlays And Distributed Systems (ROADS), Warsaw, Poland", July 2007.

[14] A. FRANCILLON, C. CASTELLUCCIA. *TinyRNG, A Cryptographic Random Number Generator for Wireless Sensor Network Nodes*, in "5th Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, IEEE WiOpt'07, Cyprus", April 2007.

[15] M. A. KAAFAR, L. MATHY, K. SALAMATIAN, C. BARAKAT, T. TURLETTI, W. DABBOUS. *Securing Internet Coordinate Embedding Systems*, in "ACM SIGCOMM, Kyoto, Japan", August 2007.

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

[17] N. MOLLER, C. BARAKAT, K. AVRACHENKOV, E. ALTMAN. *Inter-protocol fairness between TCP New Reno and TCP Westwood+*, in "NGI 2007 (Conference on Next Generation Internet Networks), Trondheim, Norway", May 2007.

[18] K. SBAI, C. BARAKAT. *Transport Information Collection Protocol with clustering of information sources*, in "NTMS 2007 (Conference on New Technologies, Mobility and Security), Paris", May 2007.

[19] T. SPYROPOULOS, T. TURLETTI, K. OBRACZKA. *Utility-based Message Replication for Intermittently Connected Heterogeneous Networks*, in "1st IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications (AOC), Helsinki, Finland", June 2007.

Internal Reports

[20] B. ADAMSON, V. ROCA. *Security and Reliable Multicast Transport Protocols: Discussions and Guidelines*, IETF RMT Working Group, Work in Progress, July 2007, http://planete.inrialpes.fr/~roca/doc/draft-ietf-rmt-sec-discussion-00.html.

[21] M. CUNCHE, V. ROCA. *Adding Integrity Verification Capabilities to the LDPC-Staircase Erasure Correction Codes*, Research Report, n^o 6125, INRIA, February 2007, http://hal.inria.fr/inria-00131002.

[22] A. KRIFA, C. BARAKAT, T. SPYROPOULOS. *Optimal Buffer Management Policies for Delay Tolerant Networks*, Technical Report, n^o inria-00196306, INRIA, December 2007 2007, http://hal.inria.fr/inria-00196306.

[23] J. LACAN, V. ROCA, J. PELTOTALO, S. PELTOTALO. *Reed Solomon Error Correction Scheme*, IETF RMT Working Group, Work in Progress, May 2007, http://www.tools.ietf.org/tools/rfcmarkup/rfcmarkup.cgi?draft=draft-lacan-rmt-fec-bb-rs-00.txt.

[24] V. ROCA, A. FRANCILLON, S. FAURITE. *TESLA source authentication in the ALC and NORM protocols*, IETF RMT Working Group, Work in Progress: <draft-msec-tesla-for-alc-norm-02.txt>, July 2007.

[25] V. ROCA, C. NEUMANN, D. FURODET. *Low Density Parity Check (LDPC) Staircase and Triangle Forward Error Correction (FEC) Schemes*, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-fec-bb-ldpc-06.txt>, May 2007.

[26] V. ROCA. *FCAST: Scalable Object Delivery on top of the ALC Protocol*, IETF RMT Working Group, Work in Progress: <draft-roca-rmt-newfcast-00.txt>, February 2007.

[27] V. ROCA. *Simple Authentication Schemes for the ALC and NORM Protocols*, IETF RMT Working Group, Work in Progress: <draft-roca-rmt-simple-auth-for-alc-norm-00.txt>, June 2007.

[28] K. SBAI, C. BARAKAT. *Experiences on enhancing data collection in large networks*, Technical Report, n^{o} inria-00140937, INRIA, April 2007, http://hal.inria.fr/inria-00140937.

[29] M. K. SBAI, C. BARAKAT, J. CHOI, A. A. HAMRA, T. TURLETTI. *BitHoc: BitTorrent for Wireless Ad Hoc networks*, Technical Report, n^{o} inria-00196313, INRIA, December 2007 2007, http://hal.inria.fr/inria-00196313.

Miscellaneous

[30] Y. SEOK, D. DUJOVNE, T. TURLETTI, P. CUENCA. *"Leader based Multicast"*, January 2007, IEEE 802.11-07/0115r1.

[31] Y. SEOK, D. DUJOVNE, T. TURLETTI, E. QI, A. S. M. WENTINK, P. CUENCA. *"Leader based Multicast"*, March 2007, IEEE 802.11-07/0115r3.

[32] Y. SEOK, D. DUJOVNE, T. TURLETTI, E. QI, M. WENTINK. *"Leader based Multicast"*, July 2007, IEEE 802.11-07/2128r0.

[33] Y. SEOK, T. TURLETTI, P. CUENCA, J. VILLALÓN, D. SHIM. *"Audio Video Multicast Protocol"*, January 2007, IEEE 802.11-07/0034r1.