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

Table of contents

1. Team

Research Scientist

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

Technical Staff

Mohamed Amine Chaoui [Expert Engineer, until June 2008]
Bilel Ben Romdhane [Associate Engineer]
Jahanzeb Farooq [Associate Engineer, until September 2008]
Lionel Giraud [Associate Engineer]
Amir Krifa [Expert Engineer, since May 2008]
Mathieu Lacage [Dream Engineer]
Thierry Parmentelat [Senior Engineer until June 2008, then Dream Engineer]

PhD Student

Sana Ben Hamida [Funding CEA LETI, since May 2008]
Mathieu Cunche [Funding ANR contract]
Diego Dujovne [Funding Argentinian Scholarship]
Aurélien Francillon [Funding Ubisec&Sens project]
Amine Ismail [Funding CIFRE Scholarship with UDcast]
Mohamad Jaber [Funding MESR Scholarship]
Mathieu Lacage [INRIA DREAM Engineer]
Imed Lassoued [Funding INRIA grant, since September 2008]
Stevens Le Blond [Funding INRIA CORDIS Scholarship]
Daniele Perito [Funding WSN4CIP IST project, since September 2008]
Naveed Bin Rais [Funding Pakistanian Scholarship]
Mohamed Karim Sbai [Funding ExpeShare project]
Mate Soos [Funding INRIA grant]
Shafqat Ur Rehman [Funding INRIA grant, since November 2008]

Post-Doctoral Fellow

Angelo Spognardi [until December 2008]

Visiting Scientist

Jari Korhonen [EPFL, Visiting PostDoc, from October 6th to October 19th, 2008]
Amine Elabidi [ENSI, Tunis, Visiting PhD student, March 2008]
Claudio Soriente [UC Irvine, USA, Visiting PhD, from October 2008 to January 2009]
Bohran Uddin [New York University, USA, Visiting PhD, from September to December 2008]

Administrative Assistant

Dominique Guédon [Sophia]
Helen Pouchot [Grenoble]

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.

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., NS), emulations (e.g., Emulab), or in the wild experimental platforms (e.g., PlanetLab). Simulations allow a fast evaluation process, fully controlled scenarios, and reproducibility. However, they lack realism and the accuracy of the models implemented in the simulators is hard to assess. Emulation allows controlled environment and reproducibility, but it also suffers from a lack of realism. Experiments allow more realistic environment and implementations, but they lack

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

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

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

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

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

Over 2008, we have kept on developping new features and enhancements for the PlanetLab software. A substantial part of our activities have been devoted to bringing the project to a more mature stage. In a first direction, we have now completed the move towards an almost full co-development model; all the OneLab-specific features have now been merged into the mainstream codebase that is located under http://svn.planet-lab.org/; the builds that are published for PlanetLab Europe, and for the general public, can and that can be found under http://build.onelab.eu/, now differ from the stock PlanetLab distribution only by a few tweaks. Secondly, we have contributed a validation framework that allows continuous integration, as daily builds now run a set of non-regression tests. Last, we have brought more general support for the underlying Linux distribution, that allows to build the software for different release levels of Fedora and CentOS. Leveraging on these contributions, we've ben ale to take an active part in the delivery of version 4.2 earlier this year, that brought man innovations to the core system, including a complete rewrite of the network isolation mechanisms (known as vnet), as well as a new module for punching holes in the slice-isolation layer (known as vsys). We are now involved in the making of version 5.0, that aims at defining a more extensible data model for handling much more heterogeneous resources.

Besides, our initial implementation of the federation code is still current, and is what the current peering link between PlanetLab Central and PlanetLab Europe is running on. On the mid-term run, there are plans to modify it so it can cope with a wider federation without needing a n-square peering scheme. This has lead us to propose a hierarchy-based variant of the current federation scheme. Other more ambitious alternatives, like the one promoted by GENI for federating testbeds beyond the PlanetLab ecosystem, are also being explored.

5.3. WSN Security Protocols

We have developped the following TinyOS modules:

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

5.4. 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.

5.5. 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.

5.6. Prototype Software

WisMon

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

Wextool

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

WiMAX NS-3

This simulation module for the ns-3 network simulator is based on the IEEE 802.16-2004 standard. It implements the PMP topology with TDD mode and aims to provide detailed and standard compliant implementation of the standard, supporting important features including QoS scheduling services, bandwidth management, uplink request/grant scheduling and the OFDM PHY layer.

BitHoc

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

6. New Results

6.1. Data Centric Networking

Participants: Chadi Barakat, Mathieu Cunche, Walid Dabbous, Diego Dujovne, Aurelien Francillon, Amine Ismail, Mathieu Lacage, Naveed Bin Rais, Vincent Roca, Karim Sbai, Thierry Turletti.

The work on data centric architectures is a follow-up and federation of three of our previous activities (adaptive multimedia transmission protocols for heterogeneous networks, data dissemination paradigms and peer-to-peer systems). We present hereafter the results obtained in 2008 in this area.

- **Application-Level Forward Error Correction Codes (AL-FEC) and their applications to broadcast/multicast systems**

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

  We have introduced in 2005 and standardized, within the IETF RMT working group, the LDPC-staircase/LDPC-triangle large block FEC codes. These specifications are now an *IETF standard ("proposed standard" maturity level), RFC 5170* [41].

  Another activity consisted in improving the erasure recovery capabilities of these codes. This has been made possible by means of a hybrid Iterative decoding/Maximum Likelihood (based on Gaussian elimination) scheme. Our LDPC codes are now *extremely close to ideal codes* in many circumstances, while keeping a high decoding speed. This work is described in [13] and [31].
- **A new File delivery application for broadcast/multicast systems**

  FLUTE has long been the one and only official file delivery application on top of the ALC reliable multicast transport protocol. However FLUTE has several limitations (essentially because the object meta-data are transmitted independently of the objects themselves, in spite of their inter-dependency), features an intrinsic complexity, and is only available for ALC. Therefore, we started the design of FCAST, a simple, lightweight file transfer application, that works both on top of both ALC and NORM, and which, furthermore, bypasses the IPR claims of Nokia with FLUTE. This work is carried out as part of the IETF RMT Working Group, in collaboration with B. Adamson (NRL) [42], [35], [34].
- **Security of the broadcast/multicast systems**

  We believe that sooner or later, broadcasting systems will require security services. This is all the more true as heterogeneous broadcasting technologies will be used, for instance hybrid satellite-based and terrestrial networks, some of them being by nature open, wireless networks (e.g., wimax, wifi). Therefore, one of the key security services is the authentication of the packet origin, and the packet integrity check. A key point is the ability for the terminal to perform these checks easily (the terminal often has limited processing and energy capabilities), while being tolerant to packet losses. The TESLA (Timed Efficient Stream Loss-tolerant Authentication) scheme fulfills these requirements. We are therefore standardizing the use of TESLA in the context of the ALC and NORM reliable multicast transport protocols, within the IETF MSEC working group [39], [38], [37], [36]. The document passed Working Group Last Call in sept-october 2008, a new revision has been submitted to answer the comments received, and a second Working Group Last Call will be issued soon. In addition, an implementation of TESLA, integrated within our FLUTE/FCAST/ALC protocol stack, has been performed, as part of the HIPCAL project.

  In parallel, we have specified the use of simple authentication and integrity schemes (i.e., group MAC and digital signatures) in the context of the ALC and NORM protocols in [43], and we are discussing security aspects in general in [25], [24], [26]. These activities are also carried out within the IETF RMT working group.

- **Authorization management in Grids**

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

- **Enhanced MAC level Encoding scheme for Mobile Satellite TV Broadcasting**

  Protection of data against long fading time is one of the greatest challenges posed by a satellite delivery system offering multimedia services to mobile devices like DVB-SH. To deal with this challenge several enhancements and modifications of the existing terrestrial mobile TV (DVB-H) physical and link layers are being considered. These solutions provide the required protection depth but they donÇt take into account the specificity of mobile handheld devices such as power consumption, memory constraints and chipsets implementation costs. In addition to our work on application level encoding schemes, we explored the design of a MAC level scheme. We have proposed an innovative algorithm (called Multi Burst Sliding Encoding or MBSE) that extends the DVB-H intra-burst (MPE-FEC) protection to an inter-burst protection so that complete burst losses could be recovered while taking into account the specificity of mobile handheld devices. Based on a clever organisation of the data, our algorithm allows to provide protection against long term fading while still using RS code implemented in DVB-H chipsets. We evaluate the performance of MBSE by both theoretical analysis as well as intensive simulations and experiments. The results also show good performance in terms of protection, battery and memory saving. The MBSE is now under standardisation and it is considered by the DVB Forum as the main solution for the DVB-SH class terminals .

- **Disruption Tolerant Networking**

  Communication networks are traditionally assumed to be connected. However, emerging wireless applications such as vehicular networks, pocket-switched networks, etc. coupled with volatile links, node mobility, and power outages, will require the network to operate despite frequent disconnections. To this end, opportunistic routing techniques have been proposed, where a node may store-and-carry a message for some time, until a new forwarding opportunity arises. Although a number of such algorithms exist, most focus on relatively homogeneous settings of nodes. However, in many envisioned applications, participating nodes might include handhelds, vehicles, sensors, etc. These various classes have diverse characteristics and mobility patterns, and will contribute quite differently to the routing process. We have addressed the problem of routing in intermittently connected wireless networks comprising multiple classes of nodes. We have shown in [6] that proposed solutions, which perform well in homogeneous scenarios, are not as competent in this setting. To this end, we proposed a class of routing schemes that can identify the nodes of highest utility for routing, improving the delay and delivery ratio by 4-5 times. Additionally, we proposed an analytical framework based on fluid models that can be used to analyze the performance of various opportunistic routing strategies, in heterogeneous settings.

  In this research area, another work focuses on efficient message delivery mechanism to enable distribution/dissemination of messages in an internet connecting heterogeneous networks and prone to disruptions in connectivity. We called our protocol MeDeHa for Message Delivery in Heterogeneous, Disruption prone Networks. MeDeHa stores data at the link layer addressing heterogeneity at lower layers (e.g., when intermediate nodes do not support higher-layer protocols). It also takes advantage of network heterogeneity (e.g., nodes supporting more than one network) to improve message delivery. Another important feature of MeDeHa is that there is no need to deploy special-purpose nodes such as message ferries, data mules, or throwboxes in order to relay data to intended destinations,

or to connect to the backbone network wherever infrastructure is available. The network is able to store data destined to temporarily unavailable nodes for some time depending upon existing storage as well as quality-of-service issues such as delivery delay bounds imposed by the application. We have evaluated MeDeHa via simulations using indoor scenarios (e.g. convention centers, exposition halls, museums etc.) and have shown significant improvement in delivery ratio in the face of episodic connectivity [22].

These works are the result of collaborations with Thrasyvoulos Spyropoulos from ETH Zurich and Katia Obraczka from University of California Santa Cruz (UCSC).

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

In [18], [19], we propose an efficient joint scheduling and drop policy that can optimize different performance metrics, such as the average delivery rate and the average delivery delay. Using the theory of encounter-based message dissemination, we first propose an optimal policy based on global knowledge about the network. Then, we introduce a distributed algorithm that collects statistics about network history and uses appropriate estimators for the global knowledge required by the optimal policy, in practice. Using simulations based on a synthetic mobility model and a real mobility trace, we show that our history-based statistical policy successfully approximates the performance of the optimal policy in all considered scenarios. At the same time, our optimal policy and its distributed variant outperform existing resource allocation schemes for DTNs, both in terms of average delivery ratio and delivery delay.

- **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 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 then 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.

  In [8] we presented a first solution to this problem that we are currently exploring further by the help of extensive simulations on more complex scenarios. Our main objective is to minimize the time to download digital contents while enforcing cooperation among peers. We observed that one can indeed realize this objective by restricting neighborhood to reduce routing overhead and to improve throughput, while establishing few connections to remote peers to improve diversity of information.

With these enhancements to BitTorrent, one can significantly improve the completion time while fully profiting from the incentives implemented in BitTorrent to enforce fair sharing.

To push our research further in this direction and to give it a practical flavor, we worked on the design and implementation of a new application that enables content sharing among spontaneous communities of mobile users using wireless multi-hop connections. Our application is called BitHoc, which stands for BitTorrent for wireless ad hoc networks. It is an open source software developed under the GPLv3 licence. A first version of BitHoc has been made public at this URL http://planete.inria.fr/bithoc. We want BitHoc to be the real testbed over which we evaluate our solutions for the support and optimization of file sharing in a mobile wireless environnement where the existence of an infrastructure is not needed. The proposed BitHoc architecture includes two principal components: a membership management service and a content sharing service. As classical tracker-based BitTorrent membership management and peer discovery are unfeasible in ad hoc networks, we design the membership management service as a distributed tracker overlay that connects peers involved in the same sharing session (see [44] for more details on how to optimally construct this membership management overlay). Using the membership information provided by the tracker overlay, the content sharing service schedules the data transfer connections among the session members by leveraging the multihop routing feature of wireless ad-hoc networks. The testbed in its current form is composed of PDAs and smartphones equipped with WIFI adapters and Windows Mobile 6 operating system.

- **Efficient Wireless LAN Protocols**

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

  We have proposed the Aggregation with Fragment Retransmission (AFR) mechanism to achieve high efficiency at the MAC layer of IEEE 802.11n [3]. In the AFR scheme, multiple packets are aggregated into and transmitted in a single large frame. If errors occur during the transmission, only the corrupted fragments of the large frame are retransmitted. An analytic model has been developed to evaluate the throughput and delay performance of AFR over noisy channels, and to compare AFR with similar schemes in the literature. Optimal frame and fragment sizes have been calculated using this model. Transmission delays are minimized by using a zero waiting mechanism where frames are transmitted immediately once the MAC wins a transmission opportunity. We prove that this mechanism achieves maximum throughput. As a complement to the theoretical analysis, we investigated by simulations the impact of AFR on the performance of realistic application traffic for diverse scenarios: TCP, VoIP and HDTV traffic. The AFR scheme described was developed as part of the 802.11n working group work. It is the result of a collaboration with Tianji Li, David Malone and Douglas Leith from Hamilton Institute in Ireland, Qiang Ni at University of Brunel, England and Yang Xiao from the Dept. of CS at University of Alabama.

  The design of efficient IEEE 802.11 physical rate adaptation algorithms is a challenging research topic and usually the issues surrounding their implementations on real 802.11 devices are not disclosed. The challenge of rate adaptation schemes is to adapt the physical transmission rate based on channel-related losses, i.e. collisions should not influence the choice of the rate. In [5] we presented a survey on existing physical rate adaptation mechanisms and discuss their advantages and drawbacks. In [20] we proposed a new rate adaptation algorithm that behaves like Auto Rate Fallback (ARF), but makes use of the RTS/CTS handshake, only when necessary, to decide whether the physical transmission rate should be changed. The main advantages of this algorithm are its simple implementation and the good performance it attains in presence of collisions. We evaluated the performance of this new algorithm and compared it with performance of other well known algorithms using the new NS-3 simulator.

6.2. Security in infrastructure-less and constrained networks

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

- **Authenticated Message Aggregation 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 data aggregation, multiple source nodes send their data to a sink along a concast tree with aggregation done en route so that the sink can obtain the aggregate (which could be the sum, average, etc.) of all these data. End-to-end privacy and aggregate integrity are the two main goals of secure data aggregation. While the privacy goal has been studied and some solutions proposed, providing end-to-end aggregate integrity in the presence of possibly compromised aggregating nodes remains largely an open problem. Message Authentication Codes (MAC) are commonly used to provide end-to-end data integrity in two party settings. Natural extensions of MAC for the data aggregation scenario are considered. It is shown that a straightforward and intuitive refinement of the MAC security model (for the data aggregation setting) is not achievable. A weaker security notion is proposed; This analysis and model is described in [12].

  During this past year, we also designed a novel secure data aggregation protocol that provides security and integrity for sensor networks using inexpensive cryptographic tools. Our scheme protects against both internal and external attackers and balances message size, as well as energy consumption among network nodes. It provides the sink with a great amount of information, as it is able to compute mean, standard deviation, frequency distribution, etc. of the sensed values, with only one query. This scheme is described in [10].

- **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, called RoK, 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 last year [11].

  During this year, the RoK was implemented under TinyOS. The research about RoK is still in progress, since several improvement are currently under investigation. A first idea is to substitute the hash chain RoK relies on, with hash tree, to reduce the storage overhead. The second idea is to

enable a self-healing mechanism between newly deployed sensors and old nodes. Preliminary results encourage to keep looking on this direction.

- **Unattended Wireless Sensor Networks**

  We studied the security problems related to the Unattended Wireless Sensor Networks (UWSN for short), in which a collector-sink is available to collect sensed data at unpredictable and irregular time intervals. During its absence, sensors must locally store data collected from the environment until next sink visit. We addressed several problems related to UWSN. In a first paper [15], [7], we envisaged and addressed the survivability of a sensible data on UWSNs operating in hostile settings where the adversary's goals and abilities are tailored to the unattended nature of the network. While the previous work focus on countermeasures that do not use any kind of cryptography, in a sequent paper [45] we propose cryptographic defenses for coping with a focused mobile adversary in UWSNs. Another problem that has been addressed is the data authentication in UWSNs [16]: namely to give the sink an effective and efficient way to establish that data gathered from the UWSN were not forged or modified by an adversary. Despite the simple network model, the issues raised in our works can pave the way for further research. This is why in future work, we plan to introduce new assumptions and variables such as communication and storage overhead, as well as new adversarial models. Moreover, the research of efficient way to detect and isolate compromised nodes seems to be an interesting and promising challenge.

- **Code Injection in Sensor Networks**

  Harvard architecture CPU design is common in the embedded world. Examples of Harvard-based architecture devices are the Mica family of wireless sensors. We show, with a practical example on the Micaz, the feasibility of remote code injection on Harvard architecture devices. This is achieved by using techniques like return oriented programming and fake stack injection in a Micaz node. We evaluate both the threat it poses to networked embedded systems (worms, botnets...) and the possible counter measures. A preliminary version of this work was presented at SSTIC [9]. The full version was presented at the ACM CCS conference [17].

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

  Code attestation in wireless sensor networks is challenging issue due to the lack of trusted hardware and the impossibility of physical access to the device. Nevertheless, without the assurance that sensors are running authentic code, reported measurements can not be trusted. Previous, software-based solutions are based on a challenge-response paradigm where the verifier challenges the sensor, to compute a checksum of its code. As the verifier knows the code running on a sensor, it compares the received checksum with a locally computed one, in order to verify the authenticity of the sensor code. Nevertheless, if a sensor running malicious code is storing the original one in its memory, a valid checksum could be still computed whenever verification is required. Proposed technique to guarantee that a compromised sensor is not storing copy of the original code, either rely on unrealistic assumptions or they just fail to take into account a broad range of malicious behaviors that a compromise node could adopt in order to deceive the verifier. Our basic idea is to verify the contents of all memories available to the sensor and to make sure that the latter has no space left where to store any code. The goal of this project is to formalize and analyze this approach and later demonstrate feasibility through implementation. Results are expected to be presented in a conference paper.

- **RFID Private Identification**

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

  We have collaborated with Karsten Nohl (University of Virginia) to break the Mifare contactless card's embedded cryptographic primitive using SAT solvers - a paper is being reviewed on this attack. We have also broken a proposed RFID private authentication protocol by Molva and Di

Pietro and published a paper about this break RFIDSec 2008 [23]. We have been developing a tool to analyse and possibly break shift-register based cryptographic algorithms.

- **Analysis and study of botnets**

  We have started an activity on Cybercriminality. We have started by studying several peer-to-peer Botnets. A botnet is a network of compromised hosts on the Internet under the control of an attacker. Botnets are considered one of the biggest threat to the proper functioning of the Internet and account for more than 90% of all spam sent everyday. We have studied a particular botnet, so called Storm. Storm uses a peer-to-peer protocol in order to coordinate the bots (the infected hosts) in the botnet Our study, led to a great understanding of the inner workings of this botnet: how it is controlled, what kind of illegal activities are conducted with it, etc. This activity is still active and should expand during the last years.

6.3. Network measurement, modeling and understanding

Participants: Chadi Barakat, Walid Dabbous, Amir Krifa, Stevens Leblond, Arnaud Legout, Emna Salhi, 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. We proposed solutions for a fast and accurate identification of Internet traffic based on packet size statistics. We also studied the feasibility of inferring path metrics as the delay and the bandwidth from indirect measurements. In the network control part, we focus on new solutions that improve the quality of service to users by a better management of network resources and by a more efficient tuning of applications that take into account the constraints posed by the network. In this direction we propose efficient message drop and scheduling mechanisms for Disruption Tolerant Networks, as well as distributed topology-aware algorithms for the scheduling of communications among members of a wireless community interested in sharing data files among each other.

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

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

  One of the most important challenges for network administrators is the identification of applications behind the internet traffic. This identification serves for many purposes as in network security, traffic engineering and monitoring. The classical methods based on standard port numbers or deep packet inspection are unfortunately becoming less and less efficient because of encryption and the utilization of non standard ports. In this work we are looking for online iterative probabilistic methods that identify applications quickly and accurately by only using statistics on the sizes of packets. We want to associate a configurable confidence level to the port number carried in the transport header and to be able to consider a variable number of packets at the beginning of a flow. After preliminary verification on real traces, we observe that even in the case of no confidence in the port number, a very high accuracy can be obtained for well known applications after few packets were examined. A paper explaining our ideas and preliminary results is currently under submission.

- **An application-aware space for enhanced scalable services in overlay networks**

  We introduce the notion of an application aware space for enhanced scalable services in overlay networks. In this new space, the proximity of peers is determined according to a utility function that considers the network parameters (e.g., delay, bandwidth, and loss rate) impacting application performance. We motivate the need for this new notion by showing that the proximity in the delay space does not automatically lead to a proximity in another space (e.g., space of the bandwidth). For determining the proximity in this new space, network parameters must be estimated easily and scalably. Therefore, we use the matrix factorization approach for estimating the delay and loss parameters. Besides, we propose a scalable model that estimates the bandwidth among peers using the bandwidth of the indirect paths that join them via a set of landmarks. Our idea is that

an indirect path shares the same tight link with the direct path with a probability that depends on the location of the corresponding landmark with respect to the direct path or any of the two peers subject to bandwidth inference. Our experimental results show that this new notion of proximity provides a much better quality than that obtained when using the delay proximity for large file transfer applications. The whole study is supported by real measurements carried out over Planetlab. The problem description and the results we obtained are summarized in [4].

- **Understanding peer-to-peer dynamics**

  This axis 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.

  Following our previous results enabling a strong understanding of the BitTorrent core mechanisms, we have explored the practical issues that arise with the deployment of BitTorrent. In particular, in [21], we have explored the impact of the piece size on the efficiency of BitTorrent. We have shown a non-trivial relationship between content size and piece size.

  We have also worked, in the context of the Ph.D. thesis of Stevens Le Blond, on how to make BitTorrent ISP friendly [30]. One major issue with BitTorrent is that is does no take into account the underlying network topology. As a consequence some specific links are overloaded, and ISPs have to block BitTorrent traffic in order to decrease the load on those links. One solution to this problem is keep the BitTorrent traffic local to each ISP, leveraging on the ISPs network topology. This notion of locality has raised a huge interest recently. However, all proposed solutions consider only moderate locality. We have explored, running extensive very large scale experiments (with up to $10\,000$ peers on Grid5000), how BitTorrent behaves with high locality values (up to 99.998%). We have shown that using such high locality values allows to reduce the cross ISP traffic up to two orders of magnitude without any significant impact of peers download completion time.

  Finally, we continue to explore the impact of BitTorrent overlay structure on its performance. In particular, we have explored the impact of the strategy to build the overlay on BitTorrent efficiency. The considered strategies are the regular one using the tracker and a gossiping one called peer exchange. In addition to those strategies, we have introduced a variant called preemption. We perform our evaluation on large scale experiments on grid5000. This work in on-going and should lead to a technical report in 2009.

6.4. Experimental Environment for future Internet architecture

Participants: Walid Dabbous, Diego Dujovne, Jahanzeb Farooq, Mathieu Lacage, Thierry Parmentelat, Bilel Ben Rhomdhanne, 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.

- **Making easier Experimentation**

Evaluation of network protocols and architectures are at the core of research and can be performed using simulations, emulations, or experimental platforms. Simulations allow a fast evaluation process, fully controlled scenarios, and reproducibility. However, they lack realism and the accuracy of the models implemented in the simulators is hard to assess. Emulation allows controlled environment and reproducibility, but it also suffers from a lack of realism. Experimentations allow more realistic environment and implementations, but they lack reproducibility and are complex to perform. Wireless experimentations are even more challenging to evaluate due to the high variability of the channel characteristics and its sensitivity to interferences. We are developing a tool called Wextool that aims to make wireless experimentations easier to perform and analyze by automating some painful and menial tasks. Wextool is a flexible and scalable open-source tool that covers all the experimentation steps, from the definition of the experiment scenario to the generation and storage of results.In this way, researchers can better concentrate his/her efforts on peculiar research and/or implementation issues related to his/her experimental scenario.

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

  Although converging towards our first stable release in june 2008 took much longer than expected, the efforts we invested in the simulation core payed off since we were able to quickly integrate major new features during july and august 2008 and release a second stable version in september 2008 which featured third-party contributions such as python bindings and the ability to run within the simulator unmodified kernel-level network stacks with the help of the Network Simulation Craddle. A third release due to become official in december 2008 contains an icmp stack we contributed in october 2008.

  In parallel to our work on the simulation core, we started the developement of a POSIX compatibility layer which allows us to run unmodified userspace socket-based applications within ns-3: early versions of this technology were demonstrated at sigcomm in august but work on this project did not stop there: we expect to be able to merge this project in ns-3 proper sometime in february 2009, once we are able to run a few non-trivial network applications such as bit-torrent clients and quagga routing daemons.

  Finally, we pursued our work on a set of MAC and PHY wimax models. With the recent emergence of broadband wireless networks, simulation support for such networks, and especially IEEE 802.16 WiMAX, is becoming a necessity. We have implemented an IEEE 802.16 WiMAX module for the ns-3 simulator. The aim is to provide a standard-compliant and well-designed implementation of this standard. Our module implements fundamental functions of the convergence sublayer (CS) and the MAC common-part sublayer (CPS), including QoS scheduling services, bandwidth request/grant mechanism, and a simple uplink scheduler. The module provides two different versions of the PHY layer. The first one is a basic PHY implementation which simply forwards bursts received by the MAC layer ignoring any underlying PHY layer details. The second one is a PHY layer based on the WirelessMAN-OFDM specification and was developed by our colleagues at LIP6, France. The MAC module currently lacks a full implementation of the classifier as well as support for fragmentation and defragmentation of PDUs. The simulation module is described in [47].

7. Contracts and Grants with Industry

7.1. Industrial contracts

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

8. Other Grants and Activities

8.1. National projects

RNRT OSCAR (2006-2008):

The Planète group was a member of the OSCAR RNRT project. This project aimed at studying the attacks against P2P overlays and their impact on the underlying network infrastructure. Planète was responsible of studying the attacks against BitTorrent and the danger those attacks could have on the underlying network infrastructure. In particular, we evaluated how by manipulating the tracker, the BitTorrent traffic could be redirected in such a way to increase significantly the load on some specific links and by how much this could harm the underling network. Extensive simulations and experimentations over Grid 5000 were run for this purpose.

The project started in April 2006 and ended in March 2008. It involved teams from both academy and industry, such as LAAS, LIP6, France Telecom, Mitsubishi, ENS Lyon and ENST Bretagne.

RNRT CMON (2009-2012):

The Planète group is a member of the CMON RNRT project which will start in February 2009 and which involves, in addition to INRIA, Thomson Paris Lab, LIP6, ENS and the Grenouille.com company. CMON stands for collaborative monitoring. It is an industrial research project that will develop the technology needed to allow end-users to collaborate in order to identify the origin and cause of Internet service degradation. The main differentiating assumptions made in this project are that (i) ISPs do not cooperate together, and (ii) one cannot rely on any information they provide in order to diagnose service problems. Even more, CMON considers that these ISP will try to masquerade the user observations in order to make their service look better. The software designed in this project will be added to the toolbox currently provided by the Grenouille project. The hope is that such a project will encourage ISPs to improve their quality of service and will contribute to improve customer satisfaction.

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

ANR/RNRT CAPRI-FEC (2007-2009):

The goal of this project is to design and analyze Application-Level FEC (AL-FEC) codes for the erasure channel, and their adequacy to wireless applications. The partners are INRIA (leader), CEA-LETI, ENSICA, STMicroelectronics, and (NAME REMOVED).

ANR/CIS HIPCAL (2007-2009):

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

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.

8.2. 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.

ITEA Expeshare (2007-2009):
Expeshare is an ITEA project to enable virtual communities to share media experiences in their personal devices legally and securely. The final aim is to develop and implement an architecture for a wireless peer-to-peer network that links personal devices and realizes DRM and mobile payment functionality and allows for legal and secure sharing of multimedia content and experiences. Over 25 European partners are involved mainly Philips, Nokia, Telefonica, VTT, the GET-INT and the university of Evry. The role of INRIA in this project is to participate to the design and evaluation of protocols for the network and Peer-to-Peer layer in order to support the sharing of media in a wireless network. We are studying the feasibility of running actual Peer-to-Peer solutions over wireless networks and trying to understand their limitations. Based on that, we are proposing new solutions to efficiently localize resources in a wireless network and to share it with other interested users. The propositions made by INRIA will be the subject of integration to modules proposed by other partners and extensive evaluation by simulation and real experimentations. The BitHoc software [32] and the research in [44], [8] give an idea on our contribution within Expeshare.

FP7 STREP ECODE (2008-2011):
ECODE is an FP7 STREP project that involves in addition to the Planète group, several European partners as Alcatel Belgium, Univ Liège, Univ of Louvain, LAAS and Univ of Lancaster. The project

started in September 2008 and will last until September 2011. ECODE stands for Experimental COgnitive Distributed Engine. The goal of the project is to develop, implement, and validate experimentally a cognitive routing system that can meet the challenges experienced by the Internet in terms of manageability and security, availability and accountability, as well as routing system scalability and quality. By combining both networking and machine learning research fields, the resulting cognitive routing system fundamentally revisits the capabilities of the Internet networking layer so as to address these challenges altogether.

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

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

8.3. INRIA supported Activities

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

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

These new highly networked environments create many new exciting security and privacy challenges. The objectives of the UbiSec associated team is to understand and tackle some of them. More specifically, the proposed project will consider the following three topics: infrastructure-less security, nano-security and anonymous association/routing. The team was prolongated for 3 years in November 2007.

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.

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. Walid Dabbous visited ENSI in December 2008 in the context of this project.

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.

9. Dissemination

9.1. Promotion of the Scientific Community

Walid Dabbous has served in the following conferences as PC member : ICC'09 CISS, GC'08 CCNS, INFOCOM'06, CoNext'05, 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). 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.

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, ACM WiSEC2008 and SecureCom2008. He has served several times as an expert to the European Commission to evaluate and review EC funded projects. He is the co-founder of the ESAS workshop and the ACM WiSec (Wireless Security) conference.

Thierry Turletti , Senior IEEE member, is in the Program Committee of the following conferences/workshops: BroadWiM'04, Packet Video'99-09, 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), the IEEE International Symposiums on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'05-07) and the 3rd International Workshop on Performance Analysis and Enhancement of Wireless Networks (PAEWN'08). 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 (WCMC) Weslay Journal published by

John Wiley & Sons. He is also part of the Editorial Board of the Journal of Mobile Communication, Computation and Information (WINET) published by Springer Science and of the Advances in Multimedia Journal published by Hindawi Publishing Corporation. 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 -). He served (is serving) on the Technical Program Committee for several conferences as Algotel 2009, ITC 2009, Infocom 2004, 2005 and 2009, Broadnets 2008, WNS2 2007 and 2008, WinMee 2008, PFLDnet 2008, SECON 2007, IMC 2005, PAM 2004 and 2005, ICNP 2002 and 2005, etc.

Chadi Barakat was invited to give talks at different places as Brunel Univ (London) 2008, 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, etc. And he presented papers at several conferences as SECON 2008 (San Francisco), CoNext 2006 (Lisboa), CoNext 2005 (Toulouse), WiOpt 2003 (Paris), PFLDnet 2003 (Geneva), IMW 2002 (Marseille), INFOCOM 2001 (Alaska), SIGCOMM 2000 (Stockholm), SIGMETRICS 2000 (Santa Clara), NETWORKING 2000 (Paris), GLOBECOM 1999 (Rio).

Chadi Barakat is member of the recruitment committee at the computer science department of the University of Nice-Sophia Antipolis, and was 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 was member of the scientific committee for the summer school RESCOM'2008, he has served as a PC member of CoNext'2008, and he is reviewer for IEEE/ACM Transactions on Networking, 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).

9.2. University Teaching

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

Understanding Networks: Course at Master IFI, University of Nice-Sophia Antipolis, by W. Dabbous and C. Barakat(42h).

Internet Measurements and Traffic Analysis: (i) Networking and Distributed Systems Master at the University of Nice Sophia Antipolis, 2004-2007, and (ii) Master RIM, ENSI, Tunis, 2003-present, by C. Barakat (15h).

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

Voice over IP: Graduate Course at (i) Master RTM of the IUP Avignon and (ii) Master TIM UNSA, by C. Barakat (7h).

Network Simulator ns-2 : 7 hours, Master RTM of IUP Avignon, 2008.

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

Networking: IUT Informatique, University Pierre Mendes France, Grenoble, by V. Roca (28h).

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

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

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

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

9.3. PhD Theses and Internships

9.3.1. HDR defended in 2008

1. Walid Dabbous defended his accreditation to supervise research (HDR) on February 2008 [2]. The title of his HDR thesis is "Quelle architecture pour l'Internet du futur?".
2. Claude Castelluccia defended his accreditation to supervise research (HDR) on September 2008 [1]. The title of his HDR thesis is "Sécurité des systèmes sans fil embarqués.".

9.3.2. PhD defended in 2008

9.3.3. Ongoing PhDs

1. Sana Ben Hamida works on "Embedded System Security".
2. Mathieu Cunche works on "Forward Error correction codes for the erasure channel ".
3. Diego Dujovne works on "Wireless Experimental Test-beds".
4. Aurélien Francillon works on "WSN security".
5. Amine Ismail works on "Optimisation of IP Protocols and Applications over Broadcast Links".
6. Mohamad Jaber works on "Detection and Troubleshooting of Internet Anomalies".
7. Mathieu Lacage works on "An IP-level network topology and link characteristic measurement tool".
8. Imed Lassoued works on "Adaptive Sampling".
9. Stevens Le Blond works on "Next Generation Peer-to-Peer Infrastructures".
10. Daniele Perito works on "Critical Infrastructure Protection".
11. Naveed Bin Rais works on "Adaptive Communication Mechanisms for Networks with Episodic Connectivity".
12. Mohamed Karim Sbai works on "Architecture for data sharing in wireless network".
13. Mate Soos works on"RFID Security".
14. Shafqat Ur Rehman works on "'Benchmarking Methodology for Network Protocols Evaluation".

9.3.4. Training activities

1. Guy Hugot-Derville worked on the impact of content size on BitTorrent efficiency. Duration of the stay: 3 months. Prepared degree: Master in Computer Sciences. Affiliation: Ecole Polytechnique, Palaiseau, France.
2. Claudio Soriente worked on code attestion. Duration of the stay: 4 months. Prepared degree: Phd Degree in Computer Science. Affiliation: University of California, Irvine.
3. Daniele Perito Duration of the stay: 6 months. Prepared degree: Master Degree in Computer Science. Affiliation: University of Roma, La Sapienza, Italy.
4. Borhan Ubbun Duration of the stay: 4 months. Prepared degree: Phd Degree in Computer Science. Affiliation: New York University, NY, USA.

10. Bibliography

Year Publications

Doctoral Dissertations and Habilitation Theses

[1] C. CASTELLUCCIA. *SÃ©curitÃ© des systÃ¨mes sans fil embarquÃ©s*, Habilitation Ã Diriger des Recherches, 2008.

[2] W. DABBOUS. *Quelle architecture pour l'Internet du futur?*, Habilitation Ã Diriger des Recherches, 2008.

Articles in International Peer-Reviewed Journal

[3] T. LI, Q. NI, D. MALONE, D. LEITH, Y. XIAO, T. TURLETTI. *Aggregation with Fragment Retransmission for Very High-Speed WLANs*, in "to appear in IEEE/ACM Transactions on Networking", April 2009.

[4] M. MALLI, C. BARAKAT, W. DABBOUS. *CHESS: An application-aware space for enhanced scalable services in overlay networks*, in "Computer Communications Journal, vol. 31, no. 6, pp. 1239-1253, April 2008".

[5] M. MANSHAEI, M. LACAGE, C. HOFFMANN, T. TURLETTI. *On Selecting the Best Transmission Mode for WiFi Devices*, in "to appear on Wireless Communications and Mobile Computing, published online July 2008", 2009.

[6] T. SPYROPOULOS, T. TURLETTI, K. OBRACZKA. *Routing in Delay Tolerant Networks Comprising Heterogeneous Node Populations*, in "to appear in IEEE Transaction on Mobile Computing", 2009.

International Peer-Reviewed Conference/Proceedings

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

[8] K. SBAI, C. BARAKAT, J. CHOI, A. A. HAMRA, T. TURLETTI. *Adapting BitTorrent to wireless ad hoc networks*, in "in proceedings of the AdHoc-Now Networks and Wireless conference, Sophia Antipolis", September 2008.

National Peer-Reviewed Conference/Proceedings

[9] C. CASTELLUCCIA, A. FRANCILLON. *Proteger les reseaux de capteurs sans fil*, in "SSTIC2008", 2008.

Workshops without Proceedings

[10] C. CASTELLUCCIA, C. SORIENTE. *ABBA: A Balls and bins approach to secure aggregation in WSNs*, in "Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, 2008. WiOPT 2008. 6th International Symposium on", April 2008, p. 185-191.

[11] C. CASTELLUCCIA, A. SPOGNARDI. *A Robust Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks*, in "IEEE Securecom'07", 2007.

[12] A.-F. CHAN, C. CASTELLUCCIA. *On the (Im)possibility of aggregate message authentication codes*, in "Information Theory, 2008. ISIT 2008. IEEE International Symposium on", July 2008, p. 235-239.

[13] M. CUNCHE, V. ROCA. *Optimizing the Error Recovery Capabilities of LDPC-staircase Codes Featuring a Gaussian Elimination Decoding Scheme*, in "10th IEEE International Workshop on Signal Processing for Space Communications (SPSC'08), Rhodes Island, Greece", October 2008.

[14] M. CUNCHE, V. SAVIN, V. ROCA, G. KRAIDY, A. SORO, J. LACAN. *Low-rate coding using incremental redundancy for GLDPC codes*, in "IEEE International Workshop on Satellite and Space Communications 2008 (IWSSC'08)", October 2008.

[15] R. DI PIETRO, L. V. MANCINI, C. SORIENTE, A. SPOGNARDI, G. TSUDIK. *Catch Me (If You Can): Data Survival in Unattended Sensor Networks*, in "IEEE PerCom'08", 2008.

[16] R. DI PIETRO, C. SORIENTE, A. SPOGNARDI, G. TSUDIK. *Intrusion-Resilience via Collaborative Authentication in Unattended WSNs*, in "ACM WiSec '09", 2009.

[17] A. FRANCILLON, C. CASTELLUCCIA. *Code injection attacks on harvard-architecture devices*, in "CCS '08: Proceedings of the 15th ACM conference on Computer and communications security, New York, NY, USA", ACM, 2008, p. 15–26.

[18] A. KRIFA, C. BARAKAT, T. SPYROPOULOS. *An Optimal Joint Scheduling and Drop Policy for Delay Tolerant Networks*, in "in proceedings of the WoWMoM Workshop on Autonomic and Opportunistic Communications, Newport Beach (CA)", June 2008.

[19] A. KRIFA, C. BARAKAT, T. SPYROPOULOS. *Optimal Buffer Management Policies for Delay Tolerant Networks*, in "in proceedings of the 5th IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 2008) - Best Paper, San Francisco", June 2008.

[20] F. MAGUOLO, M. LACAGE, T. TURLETTI. *Efficient Collision Detection for Auto Rate Fallback Algorithm*, in "3rd Workshop on multiMedia Applications over Wireless Networks, Marrakech, Morocco", July 2008.

[21] P. MARCINIAK, N. LIOGKAS, A. LEGOUT, E. KOHLER. *Small Is Not Always Beautiful*, in "In Proc. of IPTPS'2008, Tampa Bay, FL, USA", February 2008.

[22] R. B. RAIS, T. TURLETTI, K. OBRACZKA. *Coping with Episodic Connectivity in Heterogeneous Networks*, in "ACM MSWiM, Vancouver, Canada", October 2008.

[23] M. SOOS. *Analysing the Molva and Di Pietro Private RFID Authentication Scheme*, in "RFIDSec 00", 2008.

Research Reports

[24] B. ADAMSON, V. ROCA. *Security and Reliable Multicast Transport Protocols: Discussions and Guidelines*, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-sec-discussion-02.txt>, July 2008.

[25] B. ADAMSON, V. ROCA. *Security and Reliable Multicast Transport Protocols: Discussions and Guidelines*, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-sec-discussion-01.txt>, February 2008.

[26] B. ADAMSON, V. ROCA, H. ASAEDA. *Security and Reliable Multicast Transport Protocols: Discussions and Guidelines*, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-sec-discussion-03.txt>, November 2008.

[27] H. ASAEDA, K. MISHIMA, V. ROCA. *Requirements for IP Multicast Session Announcement in the Internet*, IETF RMT Working Group (individual document), Work in Progress: <draft-ietf-mboned-session-announcement-req-00>, October 2008.

[28] H. ASAEDA, K. MISHIMA, V. ROCA. *Requirements for IP Multicast Session Announcement in the Internet*, IETF RMT Working Group (individual document), Work in Progress: <draft-asaeda-mboned-session-announcement-req-00>, July 2008.

[29] C. BARAKAT, E. AL.. *TICP: TCP-friendly Information Collection Protocol*, http://www.inria.fr/planete/chadi/ticp/.

[30] S. L. BLOND, A. LEGOUT, W. DABBOUS. *Pushing BitTorrent Locality to the Limit*, Technical report, n° inria-00343822, version 1 - 2 December 2008, INRIA, December 2008.

[31] M. CUNCHE, V. ROCA. *Improving the Decoding of LDPC Codes for the Packet Erasure Channel with a Hybrid Zyablov Iterative Decoding/Gaussian Elimination Scheme*, Research Report, INRIA, March 2008, http://hal.inria.fr/inria-00263682/fr/.

[32] A. KRIFA, K. SBAI, C. BARAKAT, T. TURLETTI. *BitHoc: An Open-Source Tracker-less BitTorrent for Mobile Ad Hoc Networks*, 2008, http://planete.inria.fr/bithoc.

[33] T. PAILA, R. WALSH, M. LUBY, R. LEHTONEN, V. ROCA. *FLUTE - File Delivery over Unidirectional Transport (revised)*, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-flute-revised-06.txt>, September 2008.

[34] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, IETF RMT Working Group (individual document), Work in Progress: <draft-roca-rmt-newfcast-03.txt>, September 2008.

[35] V. ROCA, B. ADAMSON. *FCAST: Scalable Object Delivery for the ALC and NORM Protocols*, IETF RMT Working Group (individual document), Work in Progress: <draft-roca-rmt-newfcast-02.txt>, July 2008.

[36] 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-07.txt>, December 2008.

[37] 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-06.txt>, October 2008.

[38] 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-05.txt>, July 2008.

[39] 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-04.txt>, February 2008.

[40] 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-08.txt>, January 2008.

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

[42] V. ROCA. *FCAST: Scalable Object Delivery on top of the ALC Protocol*, IETF RMT Working Group (individual document), Work in Progress: <draft-roca-rmt-newfcast-01.txt>, February 2008.

[43] V. ROCA. *Simple Authentication Schemes for the ALC and NORM Protocols*, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-simple-auth-for-alc-norm-00.txt>, October 2008.

[44] K. SBAI, E. SALHI, C. BARAKAT. *Adaptive overlay for P2P membership management in MANET*, Technical Report, n^{o} inria-00342691, INRIA, November 2008.

Other Publications

[45] R. DI PIETRO, L. V. MANCINI, C. SORIENTE, A. SPOGNARDI, G. TSUDIK. *Maximizing data survival in Unattended Wireless Sensor Networks against a focused mobile adversary*, 2008, Cryptology ePrint Archive, Report 2008/293, submitted to the Elsevier journal Ad Hoc Networks.

[46] D. DUJOVNE, T. TURLETTI, W. DABBOUS. *"Experimental Methodology For Wireless Networks"*, October 2008, INRIA Research Report, RR-6667.

[47] J. FAROOQ, T. TURLETTI. *"An IEEE 802.16 WiMAX Module for the NS-3 Simulator"*, November 2008, Technical Report, inria-00336858.