INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team PLANETE

Protocoles et Applications pour l'Internet

Sophia Antipolis - Rhône-Alpes

THEME COM

Activity Report

2006

Table of contents

1. Team

Project leader
Walid Dabbous [DR, Inria]

Project coordinator in Grenoble
Claude Castelluccia [DR, Inria]

Project coordinator in Sophia
Thierry Turletti [CR, Inria, HdR]

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

Exterior collaborator
Hossam Afifi [Prof, INT Evry]

Administrative assistants
Aurélie Richard [Sophia]
Elodie Toihein [Grenoble]

Technical staff
Thierry Parmentelat [Senior Engineer]
Luc Ottavj [Senior Engineer, until November 2006]
Jahanzeb Farooq [Associate Engineer, since October 2006]

Invited Professor
Katia Obraczka [Associate Professor at University of California, Santa Cruz, since July 2006]

Post doc
Anwar Al-Hamra [since September 4th]
Chun-Fai-Aldar Chan [since September 4th]
Yongho Seok [until September 29th]
Thrasyvoulos Spyropoulos [since September 4th]

PhD students
Diego Dujovne [Funding Argentinian Scholarship]
Laurent Fazio [Funding CIFRE, ST Microelectronics, until June 2006]
Aurélien Francillon [Funding Ubisec&Sens project, since January 2006]
Mohamed Ali Kaafar [Funding RNRT Oscar]
Hahnsang Kim [Research Assistant, Imperial College London]
Zainab Khallouf [Funding CIFRE, FT R&D, until March 2006]
Mathieu Lacage [INRIA DREAM Engineer, since November 2006]
Mohamed Malli [Funding MESR until September 2006]
Mate Soos [Funding INRIA grant, since September 2006]
Abdel Basset Trad [Funding University of Nice temporary teaching contract until August 2006]

Trainees
Edmond Abboud [Master STIC RSD Sophia Antipolis, France, from January 10th 2006 to June 30th, 2006]
Mohammad Abdul Awal [AIT, Bangkok, Thailande, from February 19th, 2006 to May 19th, 2006]
Mohamed Karim Sbai [ENSI, Tunis, from March 1st, 2006 to July 1st, 2006 and since September 1st, 2006]
Medhi Msakni [ENSI, Tunis, from March 1st, 2006 to July 1st, 2006 and since October 1st, 2006]
Faouzi Kaabi [Master RSD Sophia Antipolis, France, from March 1st, 2006 to September 1st, 2006]
Youssef Zaki [Master RSD Sophia Antipolis, France, from March 1st, 2006 to September 1st, 2006]
Clément Perrin [Ecole Polytechnique, France, from April 10th 2006 to June 30th 2006]
Amaury Decreme [EPU Sophia Antipolis, France, from June 28th, 2006 to August 28th, 2006]
Masood Khosroshahy [ENST, France, from July, 1st 2006 to December 31st 2006]

Raja Mouna Abdelmoumen [SupCom, Tunis, from October 1st, 2006 to April 1st, 2006]
Mathieu Cunche [ENSIMAG, France, from March 1st to December 31st]
Nicolas Bernard [ENSIMAG, France, from March 1st to July 31st]
Jose Esparza [ENSIMAG, France, from March 1st to June 30th]
Jose Miguel Villalón [UCLM, Spain, Visiting PhD Student, until March 31st]
Niels Moller [KTH, Sweden, Visiting PhD Student, from January 16th to March 22nd]
Claudio Soriente [UC Irvine, USA, Visiting PhD Student, from September to December 2006]
Angelo Spognardi [Univ Roma, Italy, Visiting PhD Student, from September to December 2006]

2. Overall Objectives

2.1. Overall Objectives

Keywords: *Heterogeneous networks*, *communication protocols*, *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 and INRIA Rhône-Alpes research units, 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.

Mainly due to to user needs and technological improvements, the Internet witnesses an increased heterogeneity in both the network infrastructure (ATM, satellite, high speed local area networks, wireless LANs, ADSL, Mobile Ad-hoc networks, etc.) and the end hosts (fixed and mobile hosts, PCs with very significant computing capabilities, PDAs or other hand-held devices with limited CPU resources). In the same time, the introduction of new functionalities in the service provided by the inter-network layer is lacking, due to scalable deployment problems. Currently, research problems addressing secured scalable transmission protocols and adaptive mechanisms that can handle both variable network conditions and heterogeneous multimedia applications requirements are becoming crucial.

Our research projects span several areas such as security in infrastructure-less and constrained networks; scalable group communications; impact of heterogeneity on protocol performance; Internet measurement and resource localization; analysis of peer to peer protocols dynamics.

Our research activities are realized in the context of French, European and international collaborations : in particular with several academic (UCL, UCI, UCLA, MIT, UMass, Bern University, ENS, LIP6, Eurecom, INLN, etc.) and industrial (Alcatel, FT R&D, Hitachi, Intel, Motorola, Thales, Thomson Multimédia, STMicroelectronics, etc.) partners.

3. Scientific Foundations

3.1. Scientific foundations

The increased network heterogeneity raises new research topics. In this context, our project is interested in the issues related to group communications and security protocols in particular and in enhanced performance communications protocols in general. Based on a practical view, our approach 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 VTHD and PlanetLab). 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 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. We also apply technique of non-linear systems to understand the dynamics of computer network protocols. 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 to designing for security and robustness, manageability, utility and social need, new computing paradigms, integration of new network technologies, higher-level service architectures, and new theories of network architecture.

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:

- Understanding the Internet behavior;
- Seamless integration of wireless devices with the rest of network infrastructure;
- Experimental environment for future Internet architecture;
- The design of secured, privacy protecting, and robust networked systems;
- New models of information dissemination.

The following research directions are essential building blocks for the future internet architecture.

- **Network measurement, modeling and understanding**

  One topic in this area is to develop mathematically rigorous models to study and analyze the dynamics and properties of large-scale networks. One of the goals is to understand the fundamental performance limits of networks and to design algorithms that allow us to approach these limits. Another topic is to address the fundamental methodological barriers that make it hard to reproduce experiments or to validate simulations in real world systems. The goal here is to understand network behaviors for varying time-scales, a range of spatial topologies, and a range of protocol interactions. One of the major challenges with the future Internet will be how to monitor it in a scalable and distributed way. This requires designing intelligent sampling methods that provide good network coverage while reducing overhead. Another challenge will be in the characterizing of traffic sources by network operators and the detection of anomalies. The challenge for network operators in the future will be in providing an attack free Internet connectivity to their end users and in prohibiting malicious users from using their premises. A third challenge is to understand the issues related to transport and peer to peer protocols dynamics on a very large scale with the current Internet, and to propose efficient solutions for the future Internet. We describe briefly in the following the main activities in this domain.

An important objective in this domain is a better monitoring of the Internet and a better control of its resources. On one side, we focus on new measurement techniques that scale with the fast increase in Internet traffic. Among others, we use the results of measurements to infer the topology of the Internet and to localize its distributed resources. The inference of Internet topology and the localization of its resources is a building block that serves for the optimization of distributed applications and group communications. We cite in particular replicated web servers, peer-to-peer protocols and overlay routing technologies.

On the other side, we focus on solutions that optimize the utilization of network resources. Our solutions are usually based on mathematical modelling of the underlying problem and an optimization using analytical and numerical tools. This optimization is meant to provide insights on how to tune protocols and dimension networks. As examples of activities in this direction one can find the optimization of routing and its mapping to underlying layers, the dimensioning of wireless mesh networks, the clustering of network entities for the purpose for traffic collecting and monitoring, etc.

Peer to peer technology is widely widespread and highly studied. However, the dynamics of a peer-to-peer network is still not fully understood. Indeed, we observe significant differences in service capacities among the different peer-to-peer protocols. These differences are due to small protocols specificities. It is of major importance to understand why and how these specificities impact the dynamics of a peer-to-peer network. Our goal, with this new activity, is to gain a deep understanding of this dynamics in order to propose improvements for the next generation of peer-to-peer protocols.

- **Wireless Networking**

  The tremendous success of the wireless access technologies and their great diversity has further increased the heterogeneity of the Internet. The miniaturization of electronic components gave birth to a large number of new applications such as RFID, wireless sensors/nanosensors for medical applications, all kinds of wireless sensors that for example are able to avoid or forecast natural disasters, etc. Each of these new applications has particular needs and requires specific optimizations (e.g., battery life, power control to limit interferences, optimal multihop routing). These new miniaturized circuits and applications have launched the beginning of the new era of ambient networks, where the heterogeneity is more and more present. All these new applications have very different characteristics, with multiple standards, all with the same target to communicate. It is therefore important to address management and control of wireless networks including support for autoconfiguration and self-organization under policy and security constraints; creation of survivable systems in the face of the challenges of the wireless environment; issues in wireless networks from a systems perspective such as the interactions of protocol layers and different access networks including cross-layer optimizations and feedback/control mechanisms; and realistic and affordable means for carrying out representative, repeatable, and verifiable experiments to validate research on wireless networks including open tools and simulation models, as well as experimental facilities to access realistic environments and map experimental results to simulation models. We work also on how to efficiently support audio and video applications in heterogeneous wired and wireless environments. Here we focus on congestion control for multicast layered video transmission, scalable protocols for large scale virtual environments and on performance improvements and quality of service support for wireless LANs. We also consider the impact of new transmission media on the TCP protocol performance. Our goal is to provide each end user the best quality possible taking into account its varying capacities and characteristics of multimedia flows, and to propose adaptation to the TCP protocol to make it fully profit from the available resources in a heterogeneous environment.

- **Experimental Environment for future Internet architecture**

  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.

- **Security in infrastructure-less and constrained networks**

  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 interconnectivity. 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 a 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.

  Rapid advances in microelectronics are making it possible to mass-produce tiny inexpensive devices, such as processors, RFIDs, 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. Simultaneously, ad-hoc networks are gaining more and more interest in the research community. An ad-hoc network is a "spontaneous" network of wireless devices/users that does not rely on any fixed infrastructure. In such a network, each node is also a router, i.e., it routes/forwards packets for other nodes.

  Ad hoc networks can be categorized into two main groups: Mobile Ad Hoc networks (MANET) and Wireless Sensor Networks (WSN). MANETs are used to provide a communication infrastructure to end-users when an fixed infrastructure is unavailable. MANETs are typically used in emergency/rescue situations, i.e., following an earthquake, when infrastructure is destroyed. They can be also used to provide relatively cheap and flexible wireless access to network backbones. In contrast to MANETs, WSNs are not meant to provide a communication infrastructure to end-users, but rather to reach a collective conclusion regarding the environment. A WSN is typically composed of a base station (sink) and many small sensors. Communication is often one-way, i.e. only from sensors to the base stations. Even though MANETs and WSNs are closely related, they have quite different characteristics. WSNs are usually much larger than MANETs, by at least an order of magnitude. Also, WSNs act under severe technological constraints: they have severely limited computation and communication abilities. Furthermore, their power (battery) resources are limited, i.e. if a node runs out of battery power, it essentially becomes permanently non-operational. These new highly networked environments create many new exciting security and privacy challenges. Our goals are to understand and tackle some of them.

We are also interested in the particular case of RFID tag security. An RFID (Radio-Frequency IDentification) tag is a small circuit attached to a small antenna, capable of transmitting data to a distance of several meters to a reader device (reader) in response to a query. Most RFID tags are passive, meaning that they are batteryless, and obtain their power from the query signal. They is already attached to almost anything: clothing, foods, access cards and so on. Unfortunately, the ubiquity of RFID tags poses many security threats: denial of service, tag impersonation, malicious traceability, and information leakage. We focus in this work on this latter point that arises when tags send sensitive information, which could be eavesdropped by an adversary. In the framework of a library, for example, the information openly communicated by the tagged book could be its title or author, which may not please some readers. More worryingly, marked pharmaceutical products, as advocated by the US Food and Drug Administration, could reveal a person's pathology. For example, an employer or an insurer could find out which medicines a person is taking and thus work out his state of health. Large scale applications like the next generation of passports are also subject to such an issue. Avoiding eavesdropping can be done by establishing a secure channel between the tag and the reader. This requires the establishment of a session secret key, which is not always an easy task considering the very limited devices' capacities. This difficulty is reinforced by the fact that tags and reader do not share a master key in most of the applications. In the future, implementing a key establishment protocol may become a mandatory feature. For example Californian Bill 682 requires such a technical measure to be implemented in ID-cards deployed in California. RFID deployment create many new exciting security and privacy challenges. Our goals are to understand and tackle some of them.

- **New dissemination paradigms**

  The future Internet will be highly heterogeneous and should provide a scalable support for seamless information dissemination, whatever the underlying support. A lot of work has already been done on the efficient support of group communications on the Internet, both at routing, transport and application levels. These works gave birth to content broadcasting services (e.g. in DVB-H networks) as well as some content dissemination peer-to-peer systems (e.g. BitTorrent). Mastering scalable communications requires to deal with a wide range of networking components and techniques, like reliable multicast, FEC codes, multicast routing and alternative group communication techniques, audio and video coding, announcement and control protocols. Our goal in this domain is design and implement such components to ensure efficient and scalable group communications. To realise this goal, We investigate several key services and building blocks: first, the efficient application-level Forward Error Correction (AL-FEC) codes that are needed to improve the transmission reliability and application efficiency; secondly the security services (e.g. content integrity, source authentication, confidentiality) whose importance will become more and more acute especially in heterogeneous networking/broadcasting environments; and finally scalable session-level control tools that will be required to control at a high abstraction level the operational aspects of the underlying dissemination systems.

5. Software

5.1. TinyRNG

TinyRNG is an implementation of our novel Cryptographic Random Number Generator for Wireless Sensors Network Nodes under TinyOS.

This software is designed by Aurelien Francillon. It uses the noises on the wireless channel as one of the source of randomness.

5.2. MultiCast Library Version 3

MCLv3 (http://planete-bcast.inrialpes.fr/) is an implementation of the ALC (Asynchronous Layered Coding) and NORM (NACK-Oriented Reliable Multicast Protocol) content delivery Protocols, and 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. This work is done by Vincent Roca and Christoph Neumann.

5.3. LDPC large block FEC codec

Our LDPC (low-density parity-check) 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. This work is done essentially by Christoph Neumann, Vincent Roca and Aurélien Francillon. See http://planete-bcast.inrialpes.fr/ for more information.

5.4. NS-2 Simulator

NS-2 is most used simulator within the network community mainly because it implements most of network protocols and is freely available in the public domain. However, part of the simulator is very poorly written, and it is the case for the 802.11 module that does not implement rigorously the IEEE specifications. We have thus started a project to develop a new 802.11 module for ns-2 with support for several Physical layer models, multirate options for 802.11a/b and 802.11e functions to provide service differentiation. The module also contains an implementation for the classical ARF PHY rate control algorithm and the AARF improved mechanism that we have proposed previously. This work has been done by Mathieu Lacage, Dream Engineer at INRIA, in close collaboration with the NS-2 team. The new module that can be downloaded at the following URL: http://www-sop.inria.fr/planete/software/.

5.5. YANS

YANS (Yet Another Network Simulator) is a prototype network simulator that was built to experiment and validate a new core architecture and various required functionalities for network simulation. We wanted to make it very easy to perform a number of tasks which are often regarded as very hard and sometimes impossible with NS-2 or other simulators [25]. YANS is built around a C/C++ simulation core that provides a simulation event scheduler, and a number of utility APIs used to implement various network models. The rest of the C/C++ code implements models for various network components. YANS also provides a default Python wrapper for the simulation core and the models bundled with it. The code for this simulator is covered by the GPLv2 license and is available through http://yans.inria.fr/.

The YANS network simulator prototype allows us to evaluate performance of the new architecture for a possible future integration into NS-3 (http://www.nsnam.org/), the next generation of NS-2. The NS-3 four-year program funded as part of the NSF CISE CRI program was officially started on July 1, 2006 and we, and especially Mathieu Lacage, actively participate to the design choices and to the implementation of the new NS-3 simulator.

5.6. WisMon

WisMon (see URL http://www-sop.inria.fr/planete/software/WisMon/) is a wireless statistical monitoring tool. It does sniffing on the medium using a multiple probe approach. The probes synchronize the timestamp of each received packet to the beacon timestamp. This method allows the system to build a single list of packets. The captured data is processed in realtime to obtain Received Signal Strength (RSSI), inbound and outbound traffic, packet retries and transmission mode vs. time. All these parameters can be obtained in a per-station basis. The WisMon 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. The client-server approach allows the user to distribute the capture, processing and display functions into different and remote stations, provided they comply with the required network bandwidth. WisMon collects the results and simplifies parameter extraction on WLANs. It is available as open source under the Cecill license. One of the first utilization of WisMon has been to experimentally evaluate different multicast transmission mechanisms for IEEE 802.11 WLANs, see 2.

5.7. LCC Library

LCC (available through URL http://www-sop.inria.fr/planete/software/) is a two-level clustered overlay multicast architecture that aims to provide scalable, efficient and robust multicast distribution service to end users. The LCC library provides different useful application-layer functions. However, it is first designed to address topology-aware construction, so focus is set on two major processes : *Locating* and *Clustering*, see [23]. The LCC library is available as open source under the Cecill license. The LCC package also contains several test scripts such as wrappers for vic and rat MBone conferencing applications. A wrapper for vlc is under study.

5.8. Prototype Software

Intrumentation of BitTorrent

We have instrumented one of the most popular BitTorrent client in order to perform an experimental evaluation of the protocol. This instrumentation allows to log each message sent or received, and internal state of the protocol. This is the first (and only one to the date of this report) complete instrumentation of a BitTorrent client. This is a fundamental step toward the understanding of the dynamics of BitTorrent in reality. The first results obtained with this client were published in IMC'2006 [26], the best international conference on measurements. This instrumented client was publicly released in September 2006 and is available at: http://www-sop.inria.fr/planete/Arnaud.Legout/Projects/p2p_cd.html. To the date of this report this client was downloaded by the community 66 times. This instrumentation was done by Arnaud Legout.

Manet key distribution protocol

We developed a prototype software of a new key distribution protocol for adhoc networks.

6. New Results

6.1. Network measurement, modeling and understanding

Participants: Chadi Barakat, Walid Dabbous, Arnaud Legout, Mohammad Malli, Katia Obraczka, Clément Perrin, Karim Sbai, Thrasyvoulos Spyropoulos.

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. We also work on the utilization of measurements to infer the topology of the Internet and to localize any distributed resource. In the network control part, we focus on new solutions that improve the quality of service to users and that maximize the operators' revenues. Another objective is understanding the dynamics of the core mechanisms of peer-to-peer file sharing protocols. In particular, we focus on file transfer efficiency. We also want to investigate the existence and the potential impact of chaotic behaviors in the Internet. Understanding such behaviors is a scientific challenge, with the potential of a significant impact, especially concerning applications based, e.g., on chaos control, or resonances in chaotic systems.

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

- **Inferring Internet topology from application point of view**

  We introduce in this work the notion of application-level proximity that serves for enhanced scalable services in overlay networks. This new proximity definition is a function of network parameters (e.g., delay and bandwidth) that decide on the application performance. We motivate the need for this new notion by showing that the network parameters are slightly correlated. Then, we consider two typical applications: a file transfer running over the TCP protocol, and an interactive audio service. For each application, we first propose a metric that models the application quality by considering the critical network parameters (e.g., delay, bandwidth, loss rate) affecting the application performance. Then, we evaluate the enhancement of the performance perceived by peers when they choose their neighbors based on our new proximity definition instead of the delay-based one determined using the proposed utility functions. Our major contribution is a model for inferring the bandwidth among peers in an easy and scalable manner. It consists of estimating the bandwidth among peers using the bandwidth of the indirect paths that join them via a set of well defined proxies or relays that we call landmark nodes. Our idea is that an indirect path shares the same tightest 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. We evaluate the impact of the location, number, and distribution of the landmarks on the bandwidth estimation accuracy. We obtain that the application-level proximity, which is determined using our bandwidth estimation model, provides much better quality than that obtained using the delay proximity for large file transfer applications. The whole study is supported by extensive measurements carried out over the worldwide experimental network Planetlab and is published in [3], [29], [30].

- **Reformulating the Monitor Placement Problem: Optimal NetworkWide Sampling**

  Confronted with the generalization of monitoring in operational networks, researchers have proposed placement algorithms that can help ISPs deploy their monitoring infrastructure in a cost effective way, while maximizing the benefits of their infrastructure. However, a static placement of monitors cannot be optimal given the short-term and long-term variations in traffic due to rerouting events, anomalies and the normal network evolution. In addition, most ISPs already deploy router embedded monitoring functionalities. Despite some limitations (inherent to being part of a router), these monitoring tools give greater visibility on the network traffic but raise the question on how to configure a network-wide monitoring infrastructure that may contain hundreds of monitoring points. We reformulate the placement problem as follows. Given a network where all links can be monitored, which monitors should be activated and which sampling rate should be set on these monitors in order to achieve a given measurement task with high accuracy and low resource consumption? We provide a formulation of the problem, an optimal algorithm to solve it, and we study its performance on a real backbone network. This work is the result of a collaboration with Intel Research Cambridge, EPFL and Thomson. It is published in [14].

- **Modeling the AIADD Paradigm in Networks with Variable Delays**

  Modeling TCP is fundamental for understanding Internet behavior. The reason is that TCP is responsible for carrying a huge quota of the Internet traffic. During last decade many analytical models have attempted to capture dynamics and steady-state behavior of standard TCP congestion control algorithms. In particular, models proposed in literature have been mainly focused on finding relationships among the throughput achieved by a TCP flow, the segment loss probability, and the round trip time (RTT) of the connection, which the flow goes through. Recently, Westwood+ TCP algorithm has been proposed to improve the performance of classic New Reno TCP, especially over paths characterized by high bandwidth-delay products. We we developed an analytic model for the throughput achieved by Westwood+ TCP congestion control algorithm when in the presence of paths with time-varying RTT. The proposed model has been validated by using the ns-2 simulator and Internet-like scenarios. Validation results have shown that this model provides relative prediction errors smaller than 10%. It has been shown that a similar accuracy is achieved by analogous models proposed for New Reno TCP. Moreover, it has been proved that it is necessary to consider delay variability in modeling Westwood+ TCP; otherwise, if only the average RTT is considered, performance could be underestimated. All results can be found in [13]. This work was done with the Maestro group at INRIA Sophia Antipolis and with Politecnico di Bari in Italy.

- **TICP: Transport Information Collection Protocol**

  We worked on improving and validating TICP [7], our TCP-friendly reliable transport protocol to collect information from a large number of sources spread over the Internet. A collector machine sends probes to information sources, which respond by sending back report packets containing their information. TICP adapts the rate of probes in a way to avoid implosion at the collector and congestion in the network. To ensure smooth variation of the congestion control parameters and to probe sources behind the same bottleneck at the same time, we add to TICP a mechanism that clusters information sources. This mechanism is based upon the Global Network Positionning (GNP) Internet coordinate system. By running simulations in ns-2 over realistic network topologies, we prove that TICP with clustering of information sources has shorter collect session duration and causes less packet losses than the initial version that probes sources independently of their location.

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

  We started a collaboration with Pietro Michiardi and Guillaume Urvoy-Keller from the Institut Eurecom. We instrumented a BitTorrent client and performed large scale experiments to understand the dynamics of the core BitTorrent mechanisms. Such an experimental study was never performed before. Indeed, the previous studies of BitTorrent were based either on simulations or modeling; and these studies presented important restrictions. We evaluated BitTorrent's two core mechanisms: its piece selection mechanism called rarest first, and its peer selection algorithm called choke algorithm [26]. We show that the rarest first algorithm guarantees a diversity of the pieces among peers close to the ideal one. In particular, on our experiments, a replacement of the rarest first algorithm with a source or network coding solution cannot be justified. We also show that the choke algorithm in its latest version fosters reciprocation and is robust to free riders. In particular, the choke algorithm is fair and its replacement with a bit level tit-for-tat solution is not appropriate.

  Then we started a collaboration with Nikitas Liogkas, Eddie Kohler, and Lixia Zhang from UCLA, USA. Focusing on the properties of the choke algorithm [36], we show that it enables clustering of similar-bandwidth peers, ensures effective sharing incentives by rewarding peers who contribute with high download rates, and achieves high upload utilization for the majority of the download duration. We also examine the properties of the new choke algorithm in seed state and the impact of initial seed capacity on the overall BitTorrent system performance. In particular, we show that an underprovisioned initial seed does not enable clustering of peers and does not guarantee effective sharing incentives. However, we show that even in such a case, the choke algorithm guarantees an efficient utilization of the available resources by enforcing fast peers to help other peers with their download. Based on their observations, we offer guidelines for content providers regarding seed provisioning, and discuss a tracker protocol extension that addresses an identified limitation of the protocol. Those results are available in a technical report [36] that is under submission.

- **Chaotic behavior in computer networks**

Chaos is a prominent feature of complex systems and dynamical systems theory provides methods for analyzing this kind of behavior. Computer networks are complex systems, but it is not yet known whether Internet protocols exhibit chaotic behaviors though some preliminary investigations suggest it. Understanding the meaning and effect of such behaviors is a scientific challenge, with the potential of a significant impact, especially concerning applications based, e.g., on chaos control, or resonances in chaotic systems. For this, on the one hand, one needs to design models describing properly the dynamic evolution of a computer network using an Internet protocol, and to make the mathematical analysis of these models. On the other hand, one must perform careful investigations on real protocol traces, to analyze them with the tools developed in chaos theory, and to compare them to the predictions of the models. We have recently started a collaboration with researchers from the Institut Non-Linéaire de Nice (INLN) on this topic. We received a grant (COLOR CAOREDO) for one year to start this research topic, and an internship was made on that subject (Clément Perrin, 2006).

- **Disruption Tolerant Networking**

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

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

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

6.2. Wireless Networking

Participants: Anwar Al-Hamra, Chadi Barakat, Diego Dujovne, Mohamed Ali Kaafar, Mathieu Lacage, Katia Obraczka, Yongho Seok, Thierry Turletti, Jose Miguel Villalón.

- **A New MAC Scheme for Very High-Speed WLANs**
  We have studied how to improve the medium access control (MAC) layer for very high-speed Wireless LANs in order to support rich multimedia applications such as high-definition television (HDTV). We have proposed an Aggregation with Fragment Retransmission (AFR) scheme, which supports transmissions of very large frames and partial retransmissions in the case of errors. Aggregation allows increased performance despite per-transmission overhead while fragmentation alleviates the risk of losing the entire frame, a risk increases with transmission rate and frame size. Our simulations show that AFR greatly outperforms the DCF MAC protocol. In the best case we have tested, it is twice more efficient than DCF [27]. This work has been done in collaboration with several colleagues from the Hamilton Institute in Dublin, Ireland and Yang Xiao from the Univ. of Memphis, TN, USA.

- **Multicast Transmission of Multimedia Streams over WiFi**

While the deployment of WiFi networks continue to grow at an explosive rate, the multicast multimedia delivery service on WiFi compliant devices is still in its early stage of development. The real culprit is the IEEE 802.11 MAC protocol, and in particular, the absence of feedback mechanism when multicast is used. Recently, the leader-based protocol (LBP) has been proposed to overcome this problem for reliable streams. We have measured the characteristics of the legacy multicast transmission mechanism and analyze its flaws. Then, we have studied the performance of the leader-based approach and compared its performance with the standard multicast service. The analysis has been done on a large set of measurements made with our wireless testbed. Such measurements are an important complement to previous simulation studies and help in the design of the best mechanism to replace the faulty legacy multicast mechanism. Our study [18] confirms that the leader-based mechanism outperforms the standard open-loop multicast mechanism while keeping fairness among other traffic.

In parallel of this experimental study, we have designed an improved multicast transmission scheme for multimedia streams over WiFi WLANs. This scheme, called Auto Rate Selection Multicast (ARSM) aims to adapt the physical rate transmission to the varying conditions of the channel [31]. Our simulation results show that ARSF outperforms both the IEEE 802.11 standard multicast scheme and LBP.

- **Topology-Aware Overlay Multicast for Mobile Ad-Hoc Networks**
  AOMP (Ad-hoc Overlay Multicast Protocol) is a novel approach for application-layer multicast in ad-hoc networks [22]. We have designed a new algorithm that exploits a few properties of IP-routing to extract underlying topology information. The basic idea is to match path from nodes to the source in order to detect near neighbors in the physical topology. Then, in a dynamic and decentralized way, a minimum cost mobility-aware delivery tree is constructed, connecting nodes that are close to each other. We have designed a tree improvement algorithm in order to enhance the global performance of AOMP during data distribution. Our simulations results show that, compared to previously proposed application-layer multicast structures, AOMP yields trees with lower cost and traffic redundancy. In addition, it performs well in terms of packet losses, especially in case of node mobility.
- **Network Coding for Wireless Mesh Networks**
  Network coding is a new transmission paradigm that proved its strength in optimizing the usage of network resources. We have evaluated the gain from using network coding for file sharing applications running on top of wireless mesh networks. With extensive simulations carried out on a simulator we developed specifically for this study, we confirm that network coding can improve the performance of the file sharing application, but not as in wired networks. The main reason is that nodes over wireless cannot listen to different neighbors simultaneously. Nevertheless, one can get more from network coding if the information transmission is made more diverse inside the network. We support this argument by varying the loss rate over wireless links and adding more sources [19]. This work has been in collaboration with Anwar Al Hamra from Univ. of Oslo, Norway.
- **Maximizing Transfer Opportunities in Bluetooth DTNs**
  Devices in disruption tolerant networks (DTNs) must be able to communicate robustly in the face of short and infrequent connection opportunities. Unfortunately, one of the most inexpensive, energy-efficient and widely deployed peer-to-peer capable radios, Bluetooth, is not well-suited for use in a DTN. Bluetooth's half-duplex process of neighbor discovery can take tens of seconds to complete between two mutually undiscovered radios. This delay can be larger than the time that mobile nodes can be expected to remain in range, resulting in a missed opportunity and lower overall performance in a DTN. In this collaboration with the University of Massachusetts at Amherst (UMASS), we propose a simple, cost effective, and high performance modification to mobile nodes to dramatically reduce this delay: the addition of a second Bluetooth radio. We showed through analysis and simulation that this dual radio technique improves both connection frequency and duration. Moreover, despite powering two radios simultaneously, nodes using dual radios are more energy efficient, spending less energy on average per second of data transferred. We refer to [28] for more details.

- **Heterogeneous Wireless networks**

  In the context of the Divine project, we have been working on the design and evaluation through simulation of the protocols that will be developed to achieve efficient video distribution over a heterogeneous network. We have also been exploring new protocols for reliable message distribution in the face of episodic network connectivity.

  We also collaborate with Serge Fdida's group at Lip6, Paris on: (1) Self-localization in wireless sensor networks, and (2) a tool for prototyping wireless network protocols; as well as with UCSC, UCSB, and Uof Delaware on: (1) Energy-efficient MAC protocols for MANETs, (2) Sensor network systems for environmental monitoring, and (3) Robust routing for fault tolearnce and security.

6.3. Experimental Environment for future Internet architecture

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

- **Realistic Networking experimental platforms**

  The Internet is relatively resistant to fundamental change (differentiated services, IP multicast, and secure routing protocols have not seen wide-scale deployment).

  A major impediment to deploying these services is the need for coordination: an Internet service provider (ISP) that deploys the service garners little benefit until other domains follow suit. Researchers are also under pressure to justify their work in the context of a federated network by explaining how new protocols could be deployed one network at a time, but emphasizing incremental deployability does not necessarily lead to the best architecture. In fact, focusing on incremental deployment may lead to solutions where each step along the path makes sense, but the end state is wrong. The substantive improvements to the Internet architecture may require fundamental change that is not incrementally deployable.

  Network virtualisation has been proposed to support realistic large scale shared experimental facilities such as PlanetLab and GENI. We are working on this topic in the context of the European OneLab project.

  Testing on PlanetLab has become a nearly obligatory step for an empirical research paper on a new network application or protocol to be accepted into a major networking conference or by the most prestigious networking journals. If one wishes to test a new video streaming application, or a new peer-to-peer routing overlay, or a new active measurement system for geo-location of internet hosts, hundreds of PlanetLab nodes are available for this purpose. PlanetLab gives the researcher login access to systems scattered throughout the world, with a Linux environment that is consistent across all of them.

  However, network environments are becoming ever more heterogeneous. Third generation telephony is bringing large numbers of handheld wireless devices into the Internet. Wireless mesh and ad-hoc networks may soon make it common for data to cross multiple wireless hops while being routed in unconventional ways. For these new environments, new networking applications will arise. For their development and evaluation, researchers and developers will need the ability to launch applications on endhosts located in these different environments.

  It is sometimes unrealistic to implement new network technology, for reasons that can be either technological - the technology is not yet available -, economical - the technology is too expensive -, or simply pragmatical - e.g. when actual mobility is key. For these kinds of situations, we believe it can be very convenient and powerful to resort to emulation techniques, in which real packets can be managed as if they had crossed, e.g., an ad hoc network.

  In 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.

- **Enhancing network simulations**

We also need a new generation of simulation tools, that support more heterogeneous, yet closer to reality, models for links and access networks. Modelling the physical characteristics of the actual transmission media, notably for wireless networks, is required and now seems reachable for producing simulated results that would constructively complement experimental results.

We are contributing to ns3 (the future version of the ns network simulator) in order to fulfill the two following objectives: 1) the need to perform accurate experimentations in a more controlled environment than that provided by traditional testbeds such as PlaneteLab, Onelab, Emulab, or Vini. 2) the need to use accurate models of 802.11 and Wimax MAC and PHY systems to study the impact of cross-layer (Application-IP-to-MAC/PHY) optimizations, and,

1) This year, we started investigating the possibility of using simulators as a sort of super testbed where the real code written for real networks runs within the simulator. The goal of this approach is two fold: - we want to provide a more realistic environment than conventional simulations by allowing users to run the same code which runs in real networks unmodified (or minimally modified), - we want to provide a more controllable experimentation environment than conventional real-world testbeds.

To evaluate this line of research, we developed a new simulator, named YANS (see section 5.5). This initial prototype showed the feasability of the approach and we decided not to pursue the development of this tool but to contribute to the ns-3 project that was launched roughly 8 months after we started working on YANS: the stated goals of the ns-3 project are sufficiently close to those we had for YANS that we decided to contribute to the development of the ns-3 project rather than continue the development of our adhoc tool.

Since then, we have been associated to the development of the core infrastructure of the ns-3 simulator: we contributed the event scheduler and the packet data structure used in ns-3. We also contributed to the specification and refinement of the core ns-3 Node data structure. In the future, we plan to keep contributing to architectural discussions and we hope to influence the associated decisions to allow us to realize our vision of a simulator used as a more controllable real-world testbed.

2) the development of MAC/PHY models started 1.5 years ago: we developed a 802.11a/e MAC and PHY model in ns-2. This model implementation was subsequently ported to the YANS simulator [25] to validate the architecture of YANS. More recently, we started developing a Wimax MAC model for ns-3. This effort is currently focused on the identification of the components required in our model. i.e., we cannot afford to implement all of the specification given our manpower so, we need to identify the relevant components required to perform the type of application-level simulation we are interested in. In parallel to the development of this Wimax MAC model, we have started a ns-3 PHY model project which aims at defining a common API for physical layer models of signal interference and signal propagation. We plan to use the API defined within the context of this project for the above-mentioned Wimax MAC model. Furthermore, we plan to port our 802.11 MAC model to ns-3 and to the PHY-layer API of ns-3.

6.4. Security in infrastructure-less and constrained networks

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

- **TinyRNG**

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

- **Anonymous Routing**

  The need for anonymity in ad hoc networks, typically for military applications, drove several researchers to explore a wide range of techniques that aim to thwarting omni-present attackers and local attackers, given various optimization criteria such as complexity, transmission costs and processing costs.

  In the context of anonymity, the goal of an attacker is to gather as much information as possible on the network activities, namely: *who is communicating with whom?* The problem is highly relevant in ad hoc networks since the open nature of the wireless channel goes in favor of the attacker: it can eavesdrop "local" communications and gather the information from the packets themselves, or it can get a "global" view of the communications, inferring the information from the traffic patterns.

  Several techniques to improve anonymity have been proposed in the literature. They rely basically on multicast or on onion routing to thwart global attackers or local attackers respectively. None of the techniques provide a combined solution due to the incompatibility between the two components. We have developped a novel packet coding technique [12] that make the combination possible, thus integrating the advantages in a more complete and robust solution.

  Our technique has the following characteristics: (1) it combines multicast and onion-based packet encryption to provide both global and local anonymity solutions, putting the two pieces of the complete puzzle together; (2) it makes the packets, *and their headers*, change at each hop to reduce traceability. This is an inherent property of (unicast) onion routing that cannot be maintained when combined with multicast routing; (3) it leverages the wireless/open nature of the radio channel to add supporting components to make those mechanisms even more efficient in hiding network communications.

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

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

  We developped 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. We showed that aggregation based on this cipher can be used to efficiently compute statistical values such as mean, variance and standard deviation of sensed data, while achieving significant bandwidth gain.

  We have also developped AIE (Authenticated Interleaved Encryption), a new scheme that allows nodes of a network to exchange messages securely (i.e. encrypted and authenticated) without sharing a common key or using public key cryptography. This scheme is well adapted to networks, such as ad hoc, overlay or sensor networks, where nodes have limited capabilities and can share only a small number of symmetric keys. It provides privacy and integrity. An eavesdropper listening to a communication is unable to decrypt it and modify it without being detected. We show that our proposal can be used in wireless sensor networks to send encrypted packets to very dynamic sets of nodes without having to establish and maintain group keys. These sets of nodes can be explicitly specified by the source or can be specified by the network according to some criteria, such as their location, proximity to an object, temperature range. As a result, a node can, for example, send encrypted data to all the nodes within a given geographical area, without having to identify the destination nodes in advance. Finally we show that our proposal can be used to implement a secure and scalable aggregation scheme for wireless sensor networks.

- **RFID Security/Noisy Tags**

  We have developped a novel key agreement protocol that can be used between an RFID tag and a reader. Similarly to the famous blocker tag suggested by Juels, Rivest, and Szydlo, our scheme makes use of special tags that we call *noisy tags*. Noisy tags are owned by the reader's manager and set out within the reader's field. They are regular RFID tags that generate noise on the public channel between the reader and the queried tag, such that an eavesdropper cannot differentiate the messages sent by the queried tag from the ones sent by the noisy tag. Consequently, she is unable to identify the secret bits that are sent to the reader. Afterwards, the secret shared by the reader and the tag can be used to launch a secure channel in order to protect communications against eavedroppers, or it can be used to refresh securely tags' identifiers, as proposed in Molnar and Wagner's solution suited to libraries.

6.5. New Dissemination Paradigms

Participants: Walid Dabbous, Sebastien Faurite, Aurelien Francillon, Mohamed Ali Kaafar, Zainab Khallouf, Vincent Roca, Thierry Turletti.

- **Reliable multicast protocols**

  We are actively participating in the RMT working group at the IETF, and in particular on work on the FLUTE (File Delivery over Unidirectional Transport) application. FLUTE has been standardized as RFC 3926 in 2004 and is currently being revised [37], and has been included in both the 3GPP technical specification release 6 for the MBMS (Multimedia Broadcast/Multicast Service) service, and in DVB-H IP Datacasting technical specification.

  A logical and physical file aggregation scheme for FLUTE (INRIA-Nokia Internet-Draft) is currently under discussion at IETF. This is a follow up of work we started in 2004 and this should become a WG Item.

  We are also participating in the new FLUTE specifications, that take advantage of experience gained during the past two years in operational environments (3GPP and DVB-H). The goal is to move from an "Experimental" RFC to a "Proposed Standard" RFC.

- **Security in group communications**

  Security has become a major requirement, in particular in the context of Content Delivery Protocols (CDP). We are therefore working on an instantiation of the TESLA source authentication and packet integrity building block to the particular needs of the CDP, more specifically on ALC and NORM protocols [38]. We are working on an implementation of TESLA, fully integrated in our MCLv3 FLUTE/ALC and NORM library, and are standardizing this instantiation at the IETF RMT and MSEC working groups.

  Another topic is the security of the multicast routing infrastructure [1]. Multicast is a promising technology for the distribution of streaming media, bulk data and many other added-value applications. Yet the deployment of multicast still in its infancy. This work considers one of the most challenging features of multicast: the security. More specifically this thesis focusses on *the security of the multicast routing infrastructure Security from the Network Operator Point of View*. A pragmatic and easily deployable filtering solution has been designed, implemented and evaluated. This solution makes the routing infrastructure more robust to several known attacks that take advantage of group management protocols.

  Finally, we have initiated a study within the IETF that aims at analyzing the security risks associated to CDP [32]. The goals of this activity are first of all to define the possible general security goals. Defining what we want to protect, i.e. the network itself, and/or the protocol, and/or the content, is the first step; In a second step, we want to list the possible elementary security services that will make it possible to fullfil the general security goals. Some of these services are generic (e.g. object and/or packet integrity), while others are specific to RMT protocols (e.g. congestion control specific security schemes). In a third step, we want to list some technological building blocks and solutions that can provide the desired security services. Finally, we want to highlight the CDP specificities that will impact security and define some use-cases. Indeed, the set of solutions proposed to fulfill the security goals will greatly be impacted by the target use case.

- **Large block FEC codes for the erasure channel**

  Traditional small block Forward Error Correction (FEC) codes, such as the Reed-Solomon Erasure (RSE) code, are known to raise efficiency problems, in particular when applied to the ALC reliable multicast protocol. We identified a class of large block FEC codes, LDPC, capable of operating on source blocks that are several hundreds of megabytes long. We have designed an LDPC codec and performed intensive performance evaluations. We have shown that the two FEC codes we designed, LDPC-Staircase (already known in the domain) and LDCP-Triangle are significantly more interesting than Reed-Solomon codes, both in terms of raw encoding/decoding speed (they are an order of magnitude faster) and error recovery capabilities (they offer better protection with large objects).

  We are now working on the standardization of these LDPC codes at the IETF RMT Working Group [39].

  We have also proposed the use of LDPC codes in the context of the DVB-H IP Datacasting service. To that goal a DVB-H channel simulator has been designed in order to precisely benchmark these codes in a realistic environment, and compare the protection offered by our application level FEC codes with the one offered by the MPE-FEC lower level protection based on Reed Solomon codes.

  Finally, even if this is not a large block FEC codes and in spite of the associated limitations, we have participated to the standardization of Reed-Solomon codes at the IETF RMT Working Group [35]. Reed-Solomon for the erasure channel remain a technology used in the context of content broadcast.

- **DVB-SH MAC layer**

  We are working on the definition of the MAC layer of the future DVB-SH (DVB - Satellite Handheld devices) standard, meant to extend the coverage area of digital TV broadcasting systems thanks to the use of hybrid satellite/terrestrial broadcasting technics. In this context, due to the harsh packet loss conditions, the MPE-FEC MAC layer and the associated erasure correction capabilities (provided by erasure Reed-Solomon codes), designed for the particular case of DVB-H systems (terrestrial) is not sufficient. We are therefore studying new technics, based on large block codes and dispersion and/or multi MPE-frame encoding to improve the reception capabilities of mobile devices. A simulator has been designed to this purpose and results are expected soon. This is a joint work with STMicroelectronics, in close collaboration with the DVB-SH working group.

- **A Backup Tree Algorithm for Multicast Overlay Networks**

  Application Level Multicast is a promising approach to overcome the deployment problems of IP level multicast. We have developed an algorithm to compute a set of n-1 backup multicast delivery trees from the default multicast tree. Each backup multicast tree is characterized by the fact that exactly one link of the default multicast tree is replaced by a backup link from the set of available links. The trees can be calculated individually by each of the nodes. The so-called backup multicast tree algorithm can compute this set of trees with a complexity of $O(m \log n)$. This is identical to the complexity of well known minimum spanning tree algorithms. The backup multicast tree algorithm is the basis for the reduced multicast tree algorithm that can calculate a tree, which results from the default multicast tree by removing a particular node and by replacing the links of the removed node. Several mechanisms can be used to choose these explicit backup trees [8]. This work has been done in collaboration with Prof. Torsten Braun from Univ. of Bern.

- **Locate, Cluster and Conquer: A Scalable Topology-Aware Overlay Multicast**

We have designed a novel highly scalable locating algorithm for improving multicast overlay networks. Our mechanism initially directs newcomers to the closest set of existing nodes. Each newcomer sends request to a few nodes to build its neighborhood information. On the basis of the locating process, we have built a two-level topology-aware scheme, namely LCC. We have compared the scalability and efficiency of LCC with that of initially-randomly connected overlays. Results demonstrate promising performance of LCC, and show that locating-based overlays achieve 70% less link adjustments than initially randomly-connected structures, with three times faster convergence. Moreover, while being accurate, the locating process entails modest resources and incurs low overhead during new nodes arrivals [23], [24].

- **Attacks on Virtual Networks**

  The recently proposed coordinates-based systems for network positioning have been shown to be accurate, with very low distance prediction error. However, these systems often rely on nodes coordination and assume that information reported by probed nodes is correct. We have identified different attacks against coordinates embedding systems and have studied the impact of such attacks on the recently proposed Vivaldi decentralized positioning system. We made a simulation study of "genesis" attacks carried out by malicious nodes that provide biased coordinates information and delay measurement probes. We experimented with attack strategies that aim to (i) introduce disorder in the system, (ii) fool honest nodes to move far away from their correct positions and (iii) isolate a particular node in the system through collusion. Our findings confirm the susceptibility of the Vivaldi System to such attacks [20]. We have extended this work in [21] with the Sinjection T context, where the malicious nodes are introduced in the system that has already converged. This is in contrast with the Sgenesis T attack where the malicious nodes are present from the system Rs creation time. This new work not only consider Vivaldi but also NPS systems. Our study demonstrates that these attacks can seriously disrupt the operations of these systems and therefore the virtual networks and applications relying on them for distance measurements.

- **From Content Distribution Networks to Content Networks**

  In order to make multimedia content available to potentially large and geographically distributed consumer populations, Content Distribution Networks (CDNs) have been used for many years. The main task of current CDNs is the efficient delivery and increased availability of content to the consumer. Modern CDN solutions aim to additionally automate the CDN management. Furthermore, modern applications do not just perform retrieval or access operations on content, but also create and modify content, actively place content at appropriate locations of the infrastructure, etc. If these operations are also supported by the distribution infrastructure, it is called infrastructure Content Networks (CN) instead of CDN. In order to solve the major challenges of future CNs, researchers from different communities have to collaborate, based on a common terminology. In this work we have summarized the state-of-the-art, and we have identified and discussed the most important challenges for CNs [10]. Our conception of these challenges is supported by the answers to a questionnaire we received from many leading European research groups in the field. This work has been done in the context of the *E-Next* Network of Excellence (NoE) with the participation of University of Oslo, Darmstadt University of Technology, Lancaster University and Institut Eurecom.

7. Contracts and Grants with Industry

7.1. Industrial contracts

ST Microelectronics, Advanced Systems (AST), Grenoble: STM is supporting the work on LDPC codes and their use in DVB-H/SH environments.

FT R&D: France Telecom is supporting the activity on security in the network operator's multicast routing infrastructure through the PhD of Zainab Khallouf.

8. Other Grants and Activities

8.1. National projects

ACI SPLASH (2003-2006):
The goal of this protocol is to develop new security protocols for adhoc networks. The partners are Eurecom and INRIA.

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

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

RNRT DIVINE (2006-2008): The Planète group participates to the Divine ANR project on video transmission over wireless heterogeneous receivers. 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. Our first study concerns the evaluation and improvement of multicast transmission mechanism of multimedia streams over IEEE 802.11 WLANs, see 2.

COLOR CAOREDO (2006): The goal of this project is to study chaotic behaviors in computer networks. The partners are INRIA, INLN and Allot.

8.2. European projects

IST NoE E-Next (2004-2006):
is a network of Excellence grouping several teams working in the domain of networking all over Europe. We participate to the network's scientific research and dissemination activities.

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.

IST STREP OneLab (2006-2008):
Planete is part of the IST OneLab project. The goal of this project is to extend the PlanetLab to a federated model that also supports wireless access components such as UMTS and WiMax.

8.3. Associated Team

UbiSec Associated team (2005-2008): PLANETE is associated with the Secure Communication and Computing Center of UC, Irvine. The collaborative project is about wireless security.

9. Dissemination

9.1. Promotion of the Scientific Community

Walid Dabbous has served in the following conferences as PC member : Med-hoc-net' 2003, NGC'(99-2003), SAINT'2001, Networking'2000, ISCC'2000, AFRICOM'98, ICCC'97, PC co-chair of PfHSN'96, tutorial chair for Sigcomm'97, WOSBIS (97-99), CFIP (97-05), CoNext'05, INFOCOM'06. He gave several presentations and tutorials at RHDM summer school, CFIP, HPN, FORTE and ECMAST. He was co-chair of the udlr working group at the IETF between 1997 and 2000. He has served several times as an expert to the European Commission to evaluate and review EC funded projects. He has also served as an expert in RNRT commission on network protocols and architecture. He gave a presentation at the"Université de tous les savoirs" in September 2000. He also gives seminars at the technical and scientific high military education society. He is a member of the editorial board of the IEEE Communications Surveys & Tutorials electronic journal, and of a special issue of the TSI (Techniques et Sciences Informatiques) journal on the topic"Networks and protocols" (in 2004).

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

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

Chadi Barakat was general chair for PAM 2004 and WiOpt 2005 workshops, PC co-chair for the Sampling 2005 workshop, guest editor for a JSAC special issue on sampling the Internet and is area editor for the ACM CCR journal. He served in the program committees of many international conferences: SECON 2007, WWIC 2007, IWQoS 2006, WWIC 2006, WONS 2006, WiNMee 2006, IMC 2005, ICNP 2005, PAM 2005, WONS 2005, INFOCOM 2005, ASWN 2004, GI&NGN symposium at Globecom 2004, PAM 2004, INFOCOM 2004, ASIAN 2002, ICNP 2002.

Hossam Afifi has served as a TPC member in IDMS'99, TPC Chair in Globecom 2003 and several others. He is editor of the France section in the IEEE Communications Magazine. He was the creator of ASWN (Applications and Services in Wireless Networks) with Djamal Zeghlache. ASWN is a yearly IEEE sponsored workshop.

Vincent Roca was the main technical organizer of the RHDM'02 summer school, in May 2002. He organized the next International Workshop on Multimedia Interactive Protocols and Systems (MIPS) in Grenoble in 2004. He gave several tutorials in the RHDM summer schools, at ICT'03 and at MIPS'03. He is part of the Program Committee of RHDM'02, ING'03, ING'04, ING'05. He also serves as an expert in RNRT commission on network protocols and architecture in 2004, 2005 and 2006.

Arnaud Legout has served as a PC member of SIGCOMM'2007 (PC heavy), SIGCOMM'2006 (PC light), SIGCOMM'2005 (Shadow PC). He was also reviewer of journals (IEEE/ACM Transactions on Networking, IEEE/ACM Transactions on Computers, IEEE Network, Computer Communications, ACM SIGCOMM CCR), and conferences (IEEE Infocom, ACM Sigmetrics). Finally he is the organizer of the Planète Ph.D. students seminar (2005).

9.2. University Teaching

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

Networks : course at Networks and Distributed Systems graduate studies program at University of Nice-Sophia Antipolis, by W. Dabbous (24h), H. Afifi (12h).

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

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

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

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

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

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

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

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

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

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

Networks: Course 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 2006

1. Thierry Turletti defended his accreditation to supervise research (HDR) on January 2006 [5].

9.3.2. PhD defended in 2006

1. Zainab Khallouf has defended her PhD in March 2006. She studied the risks taken by a network operator that decides to deploy a multicast routing service. After a prioritization of the threats, she proposed a easy to deploy solution based on intelligent filtering of IGMP/MLD messages to mitigate some of the most easy to launch attack yet extremely efficient [1].
2. Hahnsang Kim has defended his PhD in April 2006. He worked on “Agile authentication architecture for cross-domain mobility” [2].
3. Abdel Basset Trad has defended his PhD in June 2006. His supervisor was Hossam Afifi. He worked on “Large Scale VoIP Deployment over Heterogeneous Environments” [4].
4. Mohammad Malli has defended his PhD in September 2006. He proposed a new notion of proximity for resource localization and scalable solutions to implement it. This new notion takes into account application requirements instead of simple metrics as the delay or the number of hops [3].

9.3.3. Ongoing PhDs

1. Mohamed Ali Kaafar works on “Interactive Multimedia applications on peer-to-peer networks”.
2. Diego Dujovne works on “Monitoring WiFi Networks”.
3. Mathieu Lacage works on “An IP-level network topology and link characteristic measurement tool”.
4. Aurélien Francillon works on “WSN security”.
5. Mate Soos works on “RFID Security”.

9.3.4. Training activities

1. Mohammad Abdul Awal worked on simulating voice over IP applications over ad-hoc networks. Duration of the stay: 4 months. Prepared degree: Master in Computer Sciences. Affiliation: AIT, Bangkok.
2. Amaury Decreme worked on the implementing the TICP protocol. Duration of the stay: 2 months. Prepared degree: Engineering Degree in Computer Sciences. Affiliation: EPU Sophia Antipolis.
3. Faouzi Kaabi worked on optimizing the placement of Wireless Access Points. Duration of the stay: 6 months. Prepared degree: Master RSD. Affiliation: Master RSD Sophia Antipolis.
4. Youssef Zaki worked on the design and analysis of a crawler for Bittorrent. Duration of the stay: 6 months. Prepared degree: Master RSD. Affiliation: Master RSD Sophia Antipolis.
5. Mohamed Karim Sbai worked on enhancing the TICP protocol. Duration of the stay: 10 months. Prepared degree: Engineer in Computer Sciences/Master. Affiliation: ENSI, Tunis.
6. Mehdi Msakni worked on the support of video applications over wireless networks. Duration of the stay: 9 months. Prepared degree: Engineer in Computer Sciences/Master. Affiliation: ENSI, Tunis.
7. Raja Abdelmoumen worked on the support of transport level functionalities in Delay Tolerant Networks. Duration of the stay: 6 months. Prepared degree: Engineer in Telecommunications. Affiliation: SupCom, Tunis.
8. Clément Perrin worked on an evaluation of chaotic behaviors in computer networks using simulations. Duration of the stay: 3 months. Prepared degree: Diplôme d’ingénieur. Affiliation: Ecole Polytechnique - France.
9. Edmond Abboud worked on piece selection strategies evaluation in BitTorrent. Duration of the stay: 6 months. Prepared degree: Master STIC Spécialité RSD. Affiliation:Universite Nice Sophia Antipolis.
10. Youssef Zaki worked on peer-to-peer measurements methodology. Duration of the stay: 6 months. Prepared degree: Master STIC Spécialité RSD. Affiliation:Universite Nice Sophia Antipolis
11. Mathieu Cunche worked on adding a content integrity service to LDPC FEC codes. Duration of the stay: 5 months. Prepared degree: Engineering Degree in Computer Science. Affiliation: ENSIMAG.

12. Nicolas Bernard worked on adding confidentiality to the Skype VoIP tool. Duration of the stay: 5 months. Prepared degree: Engineering Degree in Computer Science. Affiliation: ENSIMAG.
13. Jose Esparza worked on cryptographic services on small communicating sensors. Duration of the stay: 5 months. Prepared degree: Engineering Degree in Computer Science. Affiliation: ENSIMAG.

10. Bibliography

Year Publications

Doctoral dissertations and Habilitation theses

[1] Z. KHALLOUF. *Secure Multicast Routing Infrastructure: The Network Operator Point of View*, PhD thesis, Institut National Polytechnique de Grenoble, March 2006.

[2] H. KIM. *An Agile Authentication Mechanism for Inter-domain Handoffs*, PhD thesis, Institut National des Télécommunications, April 2006.

[3] M. MALLI. *Inferring Internet topology from application point of view*, PhD thesis, Université de Nice Sophia Antipolis, September 2006.

[4] A. B. TRAD. *Large Scale VoIP Deployment over Heterogeneous Environments*, PhD thesis, Université de Nice Sophia Antipolis, June 2006.

[5] T. TURLETTI. *Etude et Conception de Mécanismes pour Applications Multimédias sur Réseaux IP Filaires et Sans Fil*, Mémoire d'Habilitation à Diriger des Recherches, Université de NICE - Sophia Antipolis, January 2006.

Articles in refereed journals and book chapters

[6] P. ANSEL, Q. NI, T. TURLETTI. *FHCF: An Efficient Scheduling Scheme for IEEE 802.11e*, in "ACM/Kluwer MONET, Special Issue devoted to WiOpt R04", vol. 11, n^{o} 3, June 2006, p. 391-403.

[7] C. BARAKAT, M. MALLI, N. NONAKA. *TICP: Transport Information Collection Protocol*, in "Annals of Telecommunications, vol. 61, no. 1-2, pp. 167-192", January 2006.

[8] T. BRAUN, V. ARYA, T. TURLETTI. *Explicit Routing in Multicast Overlay Networks*, in "Computer Communications journal", vol. 29, n^{o} 12, August 2006.

[9] H. KIM, T. TURLETTI, A. BOUALI. *EPSPECTRA: A Formal Toolkit for Developing DSP Software Applications*, in "Theory and Practice of Logic Programming", vol. 6, n^{o} 4, 2006, p. 451-481.

[10] T. PLAGEMANN, V. GOEBEL, L. MATHY, T. TURLETTI, G. URVOY-KELLER. *From content distribution networks to content network-issues and challenges*, in "Computer Communications journal", vol. 29, n^{o} 5, March 2006, p. 551-562.

[11] T. TANSUPASIRI, K. KANCHANASUT, C. BARAKAT, P. JACQUET. *Using Active Networks Technology for Dynamic QoS*, in "Computer Networks, Volume 50, Issue 11", August 2006.

Publications in Conferences and Workshops

[12] I. AAD, C. CASTELLUCCIA, J. HUBAUX. *Packet coding for strong anonymity in ad hoc networks*, in "IEEE Securecomm", August 2006.

[13] G. BOGGIA, P. CAMARDA, A. RALCONZO, L. GRIECO, S. MASCOLO, E. ALTMAN, C. BARAKAT. *Modeling the AIADD Paradigm in Networks with Variable Delays*, in "proceedings of CoNEXT, Lisbon", Portugal 2006.

[14] G. R. CANTIENI, G. IANNACCONE, C. BARAKAT, C. DIOT, P. THIRAN. *Reformulating the monitor placement problem: Optimal Network-wide Sampling*, in "proceedings of CoNEXT, Lisbon", Portugal 2006.

[15] C. CASTELLUCCIA, G. AVOINE. *Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags*, in "CARDIS", April 2006.

[16] C. CASTELLUCCIA. *Authenticated Interleaved Encryption (AIE) and its applications to wireless sensor networks*, in "IACR eprint Report 2006/416", 2006, http://eprint.iacr.org/2006/416.

[17] C. CASTELLUCCIA, E. MYKLETUN, G. TSUDIK. *Re-balancing RSA-based (SSL/TLS) Handshakes*, in "ACM Asia CCS", Mars 2006.

[18] D. DUJOVNE, T. TURLETTI. *Multicast in 802.11 WLANs: An Experimental Study*, in "9-th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Torremolinos, Malaga, Spain", October 2-6 2006.

[19] A. A. HAMRA, C. BARAKAT, T. TURLETTI. *Network Coding for Wireless Mesh Networks: A Case Study*, in "IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Niagara-Falls, Buffalo-NY, USA", June 26-29 2006.

[20] M. KAAFAR, L. MATHY, T. TURLETTI, W. DABBOUS. *Real attacks on virtual networks: Vivaldi out of tune*, in "ACM SIGCOMM Workshop on Large Scale Attack Defense, Pisa, Italy", September 11-15 2006.

[21] M. KAAFAR, L. MATHY, T. TURLETTI, W. DABBOUS. *Virtual Networks under Attack: Disrupting Internet Coordinate Systems*, in "ACM/e-NEXT International Conference on Future Networking Technologies, CoNext, Lisboa, Portugal", December 2006.

[22] M. KAAFAR, C. MRABET, T. TURLETTI. *A Topology-aware overlay multicast approach for mobile ad-hoc networks*, in "Asian Internet Engineering Conference (AINTEC), Bangkok, Thailand", November 2006.

[23] M. KAAFAR, T. TURLETTI, W. DABBOUS. *A Locating-First Approach for Scalable Overlay multicast*, in "IEEE International Workshop on Quality of Service (IWQoS), New Haven, CT, USA", June 19-21 2006.

[24] M. KAAFAR, T. TURLETTI, W. DABBOUS. *Un réseau de recouvrement multipoint passant à l'échelle*, in "CFIP, Tozeur, Tunisia", October 30 - November 3 2006.

[25] M. LACAGE, T. HENDERSON. *Yet Another Network Simulator*, in "Workshop on ns-2: The IP Network Simulator, Pisa, Italy", October 2006.

[26] A. LEGOUT, G. URVOY-KELLER, P. MICHIARDI. *Rarest First and Choke Algorithms Are Enough*, in "Proc. of IMC'06, Rio de Janeiro, Brazil", October 2006.

[27] T. LI, Q. NI, D. MALONE, D. LEITH, Y. XIAO, T. TURLETTI. *New MAC Scheme for Very High-Speed WLANs*, in "IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Niagara-Falls, Buffalo-NY, USA", June 26-29 2006.

[28] M. LIBERATORE, B. LEVINE, C. BARAKAT. *Maximizing Transfer Opportunities in DTN*, in "proceedings of CoNEXT, Lisbon", Portugal 2006.

[29] M. MALLI, C. BARAKAT, W. DABBOUS. *An Enhanced Scalable Proximity Model*, in "proceedings of IEEE International Workshop on Quality of Service (IWQoS) (extended abstract), New Haven, USA", June 2006.

[30] M. MALLI, C. BARAKAT, W. DABBOUS. *Landmark-based End-to-End Bandwidth Inference*, in "proceedings of IEEE Infocom Student Workshop (extended abstract), Barcelona, Spain", April 2006.

[31] J. VILLALON, P. CUENCA, L. OROZCO-BARBOSA, Y. SEOK, T. TURLETTI. *ARSM: Auto Rate Selection Multicast Mechanism for Multi-Rate Wireless LANs*, in "I11th IFIP International Conference on Personal Wireless Communications (PWC'06), Albacete, Spain", September 20-22 2006.

Internal Reports

[32] B. ADAMSON, V. ROCA. *Security and Reliable Multicast Transport Protocols: Discussions and Guidelines*, IETF RMT Working Group, Work in Progress: <draft-adamson-roca-rmtsec-issues-00.txt>, October 2006.

[33] D. DUJOVNE, T. TURLETTI. *Multicast in 802.11 WLANs: An Experimental Study*, Research Report, n^{o} RR-5947, INRIA, May 2006, https://hal.inria.fr/inria-00084130.

[34] M. KAAFAR, L. MATHY, T. TURLETTI, W. DABBOUS. *Virtual Networks under Attack: Disrupting Internet Coordinate Systems*, Research Report, n^{o} inria-00085296 - version 1, INRIA, July 2006, https://hal.inria.fr/inria-00085296.

[35] J. LACAN, V. ROCA, J. PELTOTALO, S. PELTOTALO. *Reed Solomon Error Correction Scheme*, IETF RMT Working Group, Work in Progress: <draft-ietf-rmt-fec-bb-rs-01.txt>, June 2006.

[36] A. LEGOUT, N. LIOGKAS, E. KOHLER, L. ZHANG. *Clustering and Sharing Incentives in BitTorrent Systems*, Technical Report, INRIA, November 2006, http://hal.inria.fr/inria-00112066.

[37] 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-02.txt>, October 2004.

[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-00.txt>, June 2006.

[39] 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-03.txt>, July 2006.

[40] Y. SEOK, T. TURLETTI. *Mécanismes de Transmission Multipoint pour Réseaux Locaux Sans Fil IEEE 802.11*, Research Report, n^{o} RR-5993, INRIA, October 2006, https://hal.inria.fr/inria-00104699.