INRIA

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

2005

Table of contents

1. Team

Project leader

Walid Dabbous [DR, Inria]

Project coordinator in Grenoble

Claude Castelluccia [CR, Inria]

Project coordinator in Sophia

Thierry Turletti [CR, Inria]

Research scientists

Hossam Afifi [MdC INT Evry]
Chadi Barakat [CR, Inria]
Arnaud Legout [CR, Inria]
Vincent Roca [CR, Inria]

Administrative assistants

Aurélie Richard [Sophia]
Françoise De Coninck [Grenoble]

Technical staff

Alexis Gourdon [Expert Engineer]
Julien Labouré [Expert Engineer]
Pars Mutaf [Expert Engineer]
Christoph Neuman [Expert Engineer]
Thierry Parmentelat [Senior Engineer]

Post doc

Ceilidh Hoffmann [until March 31st]
Dongliang Guan [until October 31st]

PhD students

Lina Al-Chaal [Funding CIFRE, Netcelo]
Vijay Arya [Funding RNRT VIP]
Diego Dujovne [Funding Argentinian Scholarship]
Hossein Manshaei [Funding MESR]
Hahnsang Kim [Funding Hitachi contract]
Abdel Basset Trad [Funding RNRT VTHD++]
Laurent Fazio [Funding CIFRE, STmicro]
Zainab Khallouf [Funding CIFRE, FT R&D]
Mohamed Malli [Funding MESR]
Mohamed Ali Kaafar [Funding MUSE project]

Trainees

Mohamed ABID [ENSI, from September 15th 2004 to January 15th, 2005]
Maxime BAUDOT [ESSI, from June 27th to September 2nd, 2005]
Vincent CHARPIN [Ecole Polytechnique, from April 11th to July 13th, 2005]
Diego Roberto DUJOVNE [University of Cordoba, Argentina, from January 12th to July 12th, 2005]
Mohamed Chedly GHEDIRA [ENSI, Tunisia, from march 1st to June 24th, 2005]
Wolf Heinrich LAUPPE [Ecole Polytechnique, from April 11th to August 15th, 2005]
Farukh MUNIR [Master STIC RSD UNSA, from March 1st to August 31st, 2005]
Hangartner ROMAN [EPFL, from September 1st 2004 to February 28th, 2005]

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 internetwork 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, MIT, UMass, Bern University, ENS, LIP6, Eurecom, INLN, etc.) and industrial (Alcatel, FT R&D, Hitachi, Intel, Motorola, Thales, Thomson Multimédia, 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 (and other ad-hoc 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

We focus our work in the domains of security in infrastructure-less networks, scalable group communication, multimedia applications in heterogeneous networks, Internet measurement and resource localization, and dynamics of peer-to-peer protocols.

- **Security in infrastructure-less and constrained networks** :
  We are interested in 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, RF-IDs, sensors, and actuators. These devices are already, or soon will be, deployed in many different settings for a variety of purposes, which typically involve tracking (e.g., of hospital patients, military/rescue personnel, wildlife/livestock and inventory in stores/warehouses) or monitoring (e.g., of seismic activity, border/perimeter control, atmospheric or oceanic conditions). In fact, it is widely believed that, in the future, sensors will permeate the environment and will be truly ubiquitous in clothing, cars, tickets, food packaging and other goods.
  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): 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.
  - Wireless Sensor Networks (WSN): 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.
- **Scalable Group Communications** : 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.

- **Impact of Heterogeneity on Protocol Performance** : We work 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.
- **Internet measurement and Resource localization** : The main objective of this activity is a better monitoring of the Internet and a better localization of its resources. On one hand, we focus on new measurement techniques that scale with the fast increase in Internet traffic. On the other hand, 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.
- **Dynamics of peer-to-peer protocols** : Peer to peer technology is widely widespread and highly studied. However, the dynamic 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 dynamic of a peer-to-peer network. Our goal, with this new activity, is to gain a deep understanding of this dynamic in order to propose improvements for the next generation of peer-to-peer protocols.

5. Software

5.1. MultiCast Library

MCLv3 (http://www.inrialpes.fr/planete/people/roca/mcl/) is an Open Source Implementation of the ALC and NORM Reliable Multicast Protocols.

This software is an implementation of the two major reliable multicast protocols being standardized by the RMT IETF working group: ALC/LCT and NORM. It is composed of a C/C++ library and several applications (like FLUTE, a file transfer application over unidirectional links being standardized by the IETF) built on top of it and provides an easy-to-use and integrated solution for reliable and/or highly scalable multicast delivery of data. It is used in operational, commercial environments, essentially in the satellite broadcasting area and for file delivery over the DVB system. This work is done by V. Roca and C. Neumann.

5.2. LDPC large block FEC codec

This LDPC codec is the only Open-Source, patent free, large block FEC 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. We know several operational uses by private companies. In particular, this work has been largely supported by STmicroelectronics in 2005 and the LDPC FEC codes are currently being considered for possible standardization in the IETF and DVB-H organizations. This work is done essentially by C. Neumann, V. Roca and A. Francillon. See http://www.inrialpes.fr/planete/people/roca/mcl/ldpc_infos.html for more information.

5.3. NS-2 Simulator

NS-2 is the simulator the most used 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 PHY 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 last year [32]. This work is done in close collaboration with the NS-2 team. Mathieu Lacage, Dream Engineer at INRIA is the author of the new module that can be downloaded at the following URL: http://www-sop.inria.fr/planete/software/. The following mailing list has been set up to discuss implementation issues concerning upcoming versions of the simulator <ns-developers@ISI.EDU>.

5.4. IPv6 Opportunistic Encryption

We implemented an Opportunistic Encryption scheme for IPv6 relies on IPv6 Anycast, Authorization certificates and Crypto-Based Identifiers (CBID) to provide secure and easily deployable Opportunistic Encryption in IPv6. Unlike existing schemes (e.g. FreeS/WAN), our proposal does not rely on any global Third Trusted Party (such as DNSSEC or a PKI). Hence, we claim it is more secure, easier to deploy and more robust. We implemented our Opportunistic Encryption approach on FreeBSD 4.7. The source code will be available soon at http://www.inrialpes.fr/planete/people/chneuman/OE.html.

5.5. V-EYE

V-Eye (or Virtual-Eye) (http://www-sop.inria.fr/planete/software/V-Eye/) is a prototype application that implements a Large Scale Virtual Environment (LSVE), combining a 3D world, textual messages, multimedia communications and high definition video. When developing, our primary goal was to create a platform suitable for easily experimenting multimedia transmission, with a large number of participants, and on heterogeneous IP networks, e.g. combining a very powerful backbone such as VTHD, together with wired LANs, as well as WLANs in the IEEE 802.11 family. In particular, this platform is very useful for evaluating the scalability of transmission protocols and the support of differentiated services for multimedia applications. In this approach, agents perform a real-time mapping of the geographic area into spatial areas whose sizes depend on the density and location of participants; each of these cells is associated with a multicast group. In this way, each participant can focus on his area of interest, and receive only the relevant traffic [49].

5.6. Prototype Software

Manet key distribution protocol MANET key distribution protocol: we develop a prototype software of a new key distribution protocol for adhoc networks.

Group Member Authentication Protocol We have realized a prototype implementation of a group member authentication mechanism for MANET described in the context of a collaboration with Hitachi. Our protocol which is for secure group communication in MANET supports *knowledge-based* group member authentication which feasibly works in server-less environment. Its core technique consists of Zero Knowledge Proof (ZKP) and threshold cryptography.

6. New Results

6.1. Security in infrastructure-less and constrained networks

Participants: Claude Castelluccia, Walid Dabbous, Hossam Afifi, Hahnsang Kim, Pars Mutaf.

- **Robust Self-Keying Mobile Ad-Hoc Networks** We developed a new scheme that allows two nodes of a Mobile Ad-hoc network to compute a shared key without communicating. Such service is

important to secure routing protocols. The scheme is based on the novel combination of two well-known techniques: key pre-distribution and threshold secret sharing. Each node only needs to store a small number of keys, independent of the network size.
The proposed scheme is secure against collusion of up to a certain number of nodes. Furthermore, it is robust and DoS-resistant since a node that joins a network can efficiently verify each share it obtains from so-called authorization nodes and trace invalid shares. We evaluated and compared – via analysis and experiments – the performance of the different stages of our scheme (node join, key derivation, verification and traceability) with the performance of the Threshold-DSA based scheme proposed in the literature recently. Results clearly indicate that the new scheme is much more practical.

- **Crypto-less key exchange**
  We developed a new pairing protocol that allows two CPU-constrained wireless devices to establish a shared secret at a very low cost.
  Our scheme requires that the devices being paired, A and B, are shaken during the key exchange protocol. This is to guarantee that an eavesdropper cannot identify the packets sent by A from those sent by B. A can then send the secret bit 1 to B by broadcasting an (empty) packet with the source field set to A. Similarly, A can send the secret bit 0 to B by broadcasting an (empty) packet with the source field set to B. Only B can identify the real source of the packet (since it did not send it, the source is A), and can recover the secret bit (1 if the source is set to A or 0 otherwise). An eavesdropper cannot retrieve the secret bit since it cannot figure out whether the packet was actually sent by A or B. By randomly generating n such packets A and B can agree on a n-bit secret key.
  To our knowledge, this is the first practical pairing scheme that does not rely on expensive public-key cryptography, out-of band channels (such as a keyboard or a display) or specific hardware. The proposed protocol has very small computation and storage requirements. It is therefore well adapted to CPU-constrained devices (such as sensors) that have very limited capacities and are easy to shake.

- **Aggregation of Encrypted Data 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 developed a simple additively homomorphic stream cipher that allows efficient aggregation of encrypted data. The new cipher only uses modular additions (with very small modulo) 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.

- **IPv6 Compact neighbor discovery**
  The goal of this work is to develop new techniques to protect IPv6 Neighbor Discovery against some specific DoS attacks. The DoS attack consists of remotely flooding a target subnet with bogus packets destined for random interface identifiers; a different one for each malicious packet. The 128-bit IPv6 address reserves its 64 low-order bits for the interface ID. Consequently, the malicious packets are very likely to fall on previously unresolved addresses and the target access router (or leaf router) will be obligated to resolve these addresses by sending neighbor solicitation packets.
  Neighbor solicitation packets are link layer multicast (or broadcast), and hence also forwarded by bridges. As a consequence, the attack may consume important bandwidth in subnets with wireless bridges, or access points. This problem is particularly important in the presence of mobile IPv6 devices that expect incoming sessions from the Internet. In this case, address resolution is crucial for

the access router to reliably deliver incoming sessions to idle mobile devices with unknown MAC addresses.

We proposed a novel neighbor solicitation technique using Bloom filters. Multiple IPv6 addresses (bogus or real) in the access router's address resolution queue are compactly represented using a Bloom filter. By broadcasting a single neighbor solicitation message that carries the Bloom filter, multiple IPv6 addresses are concurrently solicited. If one (or more) of the neighbor solicitation triggering packets was legitimate, the destination host will detect its address in the received Bloom filter and return its MAC address to the access router.

A bandwidth gain around 40 can be achieved in all cells of the target subnet. This approach that we call *Compact Neighbor Discovery (CND)* is the first bandwidth DoS defense that we are aware of to employ a bandwidth optimization.

- **Secure and Robust Acknowledgment Aggregation** In certain reliable group-oriented and multicast applications, a source needs to securely verify whether all (and if not all, which) intended receivers have received a message. However, secure verification of individual acknowledgments from all receivers can impose a significant computation and communication burden. Such cost can be significantly reduced if intermediate nodes along the distribution tree aggregate acknowledgment signatures produced by many multicast receivers into a single (or few) *multisignature*.

  The approach explored in prior work is based on a multisignature scheme of which operates within so-called “Gap Diffie-Hellman” groups. Such groups and related security assumptions are fairly new. In contrast, we propose a solution using a multisignature scheme secure under more standard assumptions. In particular, we show how to extend an existing multisignature scheme to achieve both scalability and robustness. Our extension – which also generalizes to certain other multisignature schemes – allows for efficient multisignature generation even in the presence of (possibly malicious) node and communication failures.

- **RFID Security**

  An RFID (Radio-Frequency IDentification) tag is 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.

  We propose a 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.

- **Efficient Authentication for Fast Inter-domain Handoffs**
  Security concerns are of paramount importance to great gains in seamless mobility with the rapid growth of wireless device technologies. The handoff performance correlates with latency—link switch latency and network layer latency—each of which desperately demands a securing mechanism. Authentication latency has a significant impact especially on the link switch phase in the case of cross-domain mobility because of the requirement of remote contact with a home authentication server. Straightforwardly, providing a solution to minimizing the latency impact without degrading the level of security is a big challenge. In this context, we propose a high-performance authentication architecture to tackle the latency problem in cross-domain handoffs. 1) A decentralized scheme and cross-domain-supporting security protocol contribute to building the architecture. The decentralized scheme for inter-domain authentication mechanisms, i.e., peer-to-peer-based interaction between home and remote authentication servers by means of a path-traceable search, while mobiles' roam around, achieves a dramatic reduction to the authentication latency [22], as opposed to a traditional client/server model. 2) We propose a mobility-adjusted authentication protocol (MAP) dedicated to cross-domain handoffs [31], cooperating with the decentralized authentication mechanisms. The protocol leverages the concept of 'security context' to mostly avoid remote contact with the home server. It achieves a significant reduction of authentication latency without degrading the level of security.
- **Bypassing Security Model for Bluetooth Peers**
  Bluetooth technology provides conveniences ranging from simply substituting for wires of appliances to constructing home network systems. Providing Bluetooth-technology-based services in public raises security issues given unknown Bluetooth peers that intend to communicate with each other. In this context, we present a bypassing security model [30] that provides a means for secure communications between anonymous Bluetooth peers via wireless local area network and an infrastructure-based authentication scheme. The model achieves higher-performance operations on power-limited devices than a certificate-based Diffie-Hellman method.

6.2. Scalable Group Communications

Participants: Vijay Arya, Walid Dabbous, Sebastien Faurite, Aurelien Francillon, Mohamed Ali Kaafar, Zainab Khallouf, Christoph Neuman, 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 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.
  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. 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.
- **Large block FEC codes**
  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 in [51]. Our work in this domain has focused on several performance metrics : raw encoding/decoding speed of a software implementation, decoding inefficiency, and maximum memory requirements during encoding/decoding.
  We have shown that the two FEC codes we designed, LDPC-Staircase (already known in the domain) and LDCP-Triangle (that we invented) present different trade-offs, and it is therefore possible to perform the appropriate choice depending on the target environment.
  This is currently the only Open Source, patent-free, large block FEC codec available today. 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 in 2005.
  We are now working on the standardization of these LDPC codes at the IETF RMT Working Group. 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.
- **Network Tomography from Aggregate Loss Reports** Multicast applications and network monitors can potentially benefit from the ability to infer the loss rates along links within a multicast tree. Estimators, known generically by MINC, or multicast inference of network characteristics, have been developed to provide this ability. We have studied how MINC inference can, in fact, be conducted using only a default RTP packet format known as RTCP RR. RTCP RR packets contain summary information rather than per-probe information. They thus offer bandwidth savings, although this comes at the expense of an increase in estimator convergence time. Furthermore, this technique can be used by the observer of any standard RTP session, whereas estimation based upon per-probe information is only possible when a session explicitly employs the extended reporting format [27], [17]. This work has been done in collaboration with Nick Duffield from AT&T research Labs, NJ and Timur Friedman from LIP6, France.

- **Feedback Verification for Trustworthy Tomography** In network tomography tools such as MINC, certain misbehaving receivers can return incorrect feedback and mislead the MINC inference resulting in an erroneous decision. Hence it is required to verify if the feedbacks collected from the receivers can be utilized to make a trustworthy MINC inference. We have developed a MINC inference procedure to compute the loss probabilities of various paths in the multicast tree is investigated. This statistical detection procedure searches for loss probability inconsistencies in the feedback data [18].
- **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 [21]. This work has been in collaboration with Prof. Torsten Braun from Univ. of Bern.
- **Encodings of Multicast Trees** We have proposed efficient ways of encoding multicast trees. Multicast tree encodings provide a convenient way of performing stateless and explicit multicast routing in networks and overlays. We have shown the correspondence of multicast trees to theoretical tree data structures and have provided lower bounds on the number of bits needed to represent multicast trees. Our encodings can be used to represent multicast trees using both node identifiers and link indexes and are based on balanced parentheses representation of tree data structures. These encodings are almost space optimal and can be read and processed efficiently. We have evaluated the length of these encodings on multicast trees in generated and real topologies [19] This work has been done in collaboration with Shivkumar Kalyanaraman from RPI.
- **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 [43].
- **Secured Application Level Multicast** We have worked in collaboration with STmicro on the design of a protocol to transport real-time flows efficiently from few sources to a set of receivers, knowing that the number of source is limited compared to the number of receivers. As the native multicast technology is not available everywhere, the protocol is based on an overlay multicast approach..

  This protocol proposes to find a trade off between the security concerns and the constraints imposed by real-time flows. Security features are time consuming, whereas real-time flows must be delivered to applications with accurate timings. The main idea of this protocol is thus to minimize the impact of security features while decreasing the overall latency induced by the number of hops before reaching the farthest peers in the distribution tree.

  This protocol considers the followings security issues: (1) secrecy in communications (2) the integrity of data that are transported, (3) the proof of origin and (4) anti-collusion mechanisms.

Authentication is done at the root of the tree by a white list for friend peers. This functionality can be put in an authenticated server.

Instead of just using network metrics, such as round trip time and jitter to determine the position of a peer in the distribution tree, we consider using also application metrics. The main idea is to impact the shape of the distribution tree established by the Application Level Multicast protocol according to the application request. As we consider transporting real-time flows, the application needs to decrease the maximum depth of the tree, in order to decrease the overall latency between the sender and the farther peers in the distribution tree.

We are implementing this protocol in a simulator and in a real videoconferencing application.

6.3. Impact of Heterogeneity on Protocol Performance

Participants: Vijay Arya, Chadi Barakat, Gion Reto Cantieni, Mathieu Lacage, Mohammad Malli, Hossein Manshaei, Thierry Turletti.

- **Performance Analysis of the IEEE 802.11 MAC and Physical Layer Protocol**
  We have developed an analytical model that accounts for the positions of stations with respect to the Access Point (AP) while evaluating the performance of 802.11 MAC layer. In our model, given the position of one station, we compute its saturation throughput while conditioning on the positions of the other concurrent stations. Further, our model provides the total saturation throughput of the medium. We have shown that the saturation throughput per station is strongly dependent not only on the station's position but also on the positions of the other stations. Our model is helpful to dimension 802.11 wireless access networks and to study their capacities and their performances [35].
- **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 [46]. 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.
- **Closed-Loop Adaptive Rate Allocation for IEEE 802.11 WLANs**
  We have designed a closed-loop, dynamic rate adaptation algorithm called CLARA that can be implemented in all IEEE 802.11 a/b/g compliant wireless local area networks. Our proposed algorithm is a culmination of the best attributes of the transmitter-based Auto-Rate Fall-back (ARF) and the Receiver-based Auto-Rate (RBAR) control mechanisms with additional practical features to facilitate multipath fading channel sensing and feedback control signalling. Our proposed scheme is transparent in the sense that devices using our technique can co-exist with other 802.11-compliant devices in the same basic service area. By combining RTS/CTS handshake with data fragmentation, we differentiate data loss (and reduction in goodput) due to MAC collision from data corruption due to bad physical channel state and poor rate selection [28].
- **Media-Oriented Rate Selection Algorithm for Multimedia Transmission in Wireless LANs**
  We have also studied mechanisms to improve the effective throughput for transporting loss-tolerant multimedia traffic over a WLAN. The idea is to take into account both the application characteristics and the physical channel conditions to select the physical transmission mode. We have designed a media-oriented mechanism for selecting the appropriate transmission mode in 802.11-based wireless

LANs. In particular, the proposed cross-layer mechanism exploits the robustness of multimedia coding by allowing packets with corrupted payloads reach the receiving application. The results indicate that the proposed cross-layer approach achieves up to 5Mbps increase in throughput and 20-meter increase in the coverage range. Furthermore, by disabling FEC from some of the standard transmission modes, we have shown that the goodput of loss-tolerant applications can be improved significantly [9]. This work has been done in collaboration with the TEMICS group at IRISA.

- **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 [42]. This work has been in collaboration with Anwar Al Hamra from Univ. of Oslo, Norway.
- **Analysis of TCP Westwood+ in high speed networks**
  In this ongoing joint activity with the Maestro group at INRIA Sophia Antipolis, KTH (Royal Institute of Technology) in Sweden, and Politecnico di Bari in Italy, we study the performance of the Westwood+ TCP version that revealed to be particularly useful in scenarios affected by losses due to unreliable links. We focus on a single connection traversing a long wireless link (such as satellite links). The latter is characterized by random losses which are due to the noise on the channel rather than congestion, and where the round trip time has large (random) variability (e.g. due to link layer features such as the ARQ) which are again not directly related to congestion. Our modeling approach is based on [16] which, unlike many other models, takes explicitly into account the impact of delay variability on the TCP connection. This feature of the model is needed when considering Westwood+, since the window size of TCP Westwood+ is set after a loss event as a function of the estimated bandwidth delay product. With our approach we are able to show how well the slow start threshold estimator in TCP westwood+ adapts to variability in the round-trip time on high speed links.
- **Capacity Evaluation of VoIP in IEEE 802.11e WLAN Environment**
  Wireless Local Area Networks (WLANs) will need to support a large number of concurrent VoIP communications since VoIP is spreading rapidly especially in public spaces. This motivation led us to study the VoIP capacity in IEEE 802.11e WLAN and to investigate increasing this capacity by reducing VoIP codec rate while maintaining an overall good quality. We have proposed an analytical model for VoIP capacity for the upgrade version of IEEE 802.11e MAC. We have studied the effect of varying voice codec rate jointly with the durations of SF (SuperFrame) and CP (Contention Period) on the number of simultaneously supported VoIP calls. We have illustrated performance results relative to typical codec rates of G.711 PCM (64 kbit/s), G.729 (8 kbit/s) and G.723.1 (6.3 kbit/s). G.729 and G.723.1 allow a greater capacity than G.711 which is constrained by throughput. This greater capacity is at the expense of small quality degradation due to the delay increase since G.729 and G.723.1 codecs are more delay sensitive than G.711. In a second part of our study we have analyzed the occurrence of CAPs (Controlled Access Periods) during the Contention Period (CP) and its effect of a promising increase in the VoIP over WLAN capacity while keeping a low voice delay. We also showed that recent technologies such as IEEE 802.11a with high high data rates (up to 54 Mb/s) allow important VoIP capacity (up to 400 G.711 VoIP calls, 997 G.729 VoIP calls and 1045 G.723.1 VoIP calls).

- **Multicast routing protocols support in Access Networks**
  We have done in the context of the Muse European project a study on the support of multicast routing protocols in multiservice access networks. Multicast traffic support can be done at the application level, at the network level or on both levels using a hybrid approach. On the other hand, the source of the multicast traffic can be either in the network or at one of the end users of the access network. The main question here is whether the operator network should be involved in controlling/optimising the multicast traffic. It is clear that adequate mechanisms will have to be implemented only if this traffic is expected to be an important part of the supported traffic, otherwise this traffic should be dealt with at the application level. Another approach is to have a dedicated server in the access network to provide the stream duplication/mixing service for multicast traffic, if there is enough value to support investment in the network. A third approach is let the users exploit the underlying multicast support provided by the network. All these approaches were studied from general architecture perspective and adequate network level solutions discussed.
  An important aspect appears when it is envisaged to run multicast protocols in the user “home” network. This can results in “security attacks” due to malicious and/or non expert users who could run or configure the multicast protocols in such a way that jeopardize the correct functioning of the multicast protocols in the access network. An analysis of these attacks was done in collaboration with FT R& D and the adequate protection mechanisms proposed.
- **Enhancing experimental platforms**
  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 a 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.
  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.

6.4. Internet Measurement and Resource Localization

Participants: Chadi Barakat, Walid Dabbous, Mohammad Malli.

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

- **Ranking flows from sampled traffic**:
  Most of the theoretical work on packet sampling has addressed the inversion of general traffic properties such as flow size distribution, average flow size, or total number of flows. In this work published in [20] and done in collaboration with Intel Research Cambridge, we make a step towards understanding the impact of packet sampling on individual flow properties. We study how to detect and rank the largest flows on a link. To this end, we develop an analytical model that we validate on real traces from two networks. First we study a *blind* ranking method where only the number of sampled packets from each flow is known. Then, we propose a new method, *protocol-aware* ranking, where we make use of the packet sequence number (when available in transport header) to infer the number of non-sampled packets from a flow, and hence to improve the ranking. Surprisingly, our analytical and experimental results indicate that a high sampling rate (10% and even more depending on the number of top flows to be ranked) is required for a correct blind ranking of the largest flows. The sampling rate can be reduced by an order of magnitude if one just aims at detecting these flows or by using the protocol-aware method.
- **TICP: Transport Information Collection Protocol** In this work done in collaboration with Hitachi and published in [4], we develop and validate TICP, a TCP-friendly reliable transport protocol to collect information from a large number of sources spread over the Internet. TICP is a stand-alone protocol that can be used by any application requiring the reliable collection of information. It ensures two main functions: (i) the information arrives at the collector entirely and correctly, (ii) the implosion at the collector and the congestion of the network are avoided. The congestion control in TICP is done by having the collector probe the sources at a rate function of network conditions. The probing rate increases and decreases in a way similar to how TCP adapts its congestion window. We implement TICP in ns-2 and validate its performance. In particular, we show how efficient TICP is in quickly and reliably collecting information from a large number of sources, while avoiding network congestion and being fair with competing traffic.
- **Using Active Networks Technology for Dynamic QoS** This work is done in collaboration with the Asian Institute of Technology in Bangkok and the Hypercom project at INRIA. We propose a dynamic QoS, or D-QoS, model where QoS settings can be automatically reconfigured based upon requests from authorized users. Different levels of privilege can be assigned to users enabling higher privileged users to interrupt the network flows belonging to those of lower privileged levels. To request for a special QoS treatment, a user can issue an active packet to interrupt any active node along its flow path which is D-QoS enabled. The request for a specific interruption level is approved by a D-QoS enabled node which allows for multi-level interruptions to be handled. After an interrupting flow has completed transmitting all its packets, D-QoS enabled node can resume its services for those pending flows which are of lower privilege levels. In [15], we describe the overall concept of D-QoS and demonstrate how it can be implemented by a small prototype. Using simulation, we show that the proposed system can provide assurance for privileged flows with an improved network utilization where bandwidth is shared among the flows according to the levels of privilege. D-QoS should be deployed on those bottleneck hops with limited bandwidth on the edge network to ensure the best service is given to privileged users.
- **Application-level versus Network-level Proximity** We motivate in [34] the need for application-level proximity. This proximity is a function of network characteristics that decide on the application performance. Most of existing protocols rely on the network-level proximity as for example the one based on the delay (e.g., the delay closest peer is the best peer to contact). We study how much the two proximity definitions differ from each other. The work in [34] consists of running extensive measurements over the PlanetLab overlay network and comparing different proximity definitions. Our major observation is that the delay proximity is not always a good predictor of quality and that other network parameters are to be considered as well based on the application requirements.

Particulary, the best peer to contact is not always the delay closest one. This can be explained by our other observation, that of the slight correlation of network characteristics with each other

6.5. Understanding peer-to-peer dynamics

Participants: Arnaud Legout, Guillaume Urvoy-Keller, Pietro Michiardi.

The aim of this activity is to understand the dynamics of the core mechanisms of peer-to-peer file sharing protocols. In particular, we focus on file transfer efficiency.

Arnaud Legout has started a collaboration with Pietro Michiardi and Guillaume Urvoy-Keller from the Institut Eurecom. They have 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 found, during this study, four important results. First, we shown that the choke algorithm in leecher state leads to a stable equilibrium that is efficient. Second, the choke algorithm in seed state is robust to free riders; and it improves the entropy of the pieces of content. These results are important because the choke algorithm is a simple distributed algorithm. It can be applied in many other distributed context to perform an efficient peer selection. Third, the rarest first algorithm suppresses the last pieces problem, which is frequent in peer-to-peer protocols. Fourth, the rarest first algorithm guarantees a good entropy of the pieces. These results are important because a simple distributed piece selection strategy guarantees that each peer will have interesting pieces for any other peer with a high probability.

These results are detailed in a technical report [45] that is under submission.

6.6. Chaotic behavior in computer networks

Participant: Arnaud Legout.

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.

7. Contracts and Grants with Industry

7.1. Industrial contracts

Alcatel The Planète group had a collaboration of one year with Alcatel Marcoussis on Inferring the topology of the Internet. The collaboration ended in May 2005 and two researchers from Planète were involved in it, Chadi Barakat and his PhD student Mohammad Malli. From Alcatel side, Olivier Marcé was involved. This collaboration resulted in a new definition of proximity that accounts for application requirements. The motivation for this new definition and details on what it consists in were published in [34], [33].

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

ST Microelectronics, Advanced Systems: a 3 year contract has been set up (2003-2006) for Laurent Fazio's PhD on Secured Large scale virtual environments (CIFRE scholarship).

8. Other Grants and Activities

8.1. National projects

ACI SPLASH (2003-2006):
The goal of this project is to study and develop some secure routing protocols for ad-hoc networks. The partners are Eurecom and INRIA.

RNRT OSCAR (2006-2007): The Planète group was involved in the preparation of an RNRT project on the detection of overlay traffic by a network operator and the isolation of this traffic if it looks abnormal. The project is accepted and expected to start by January 2006. Planète will collaborate within this project with excellent teams from both academy and industry as LAAS, LIP6, France Telecom, Mitsubishi, ENS Lyon and ENST Bretagne.

RNRT DIVINE (2006-2007): The Planète group was also involved in the preparation of an RNRT project on video transmission over wireless heterogeneous receivers. The project should start at the beginning of 2006 and involves well-known 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.

8.2. European projects

IST IP MUSE (2004-2005):
The goal of this project is to study and develop residential gateway for future MultiService Access Networks. Our contribution in this project concentrated on multicast routing protocols support in such network architecture. The main contractor is Alcatel.

IST NoE E-Next (2004-2005):
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&Sen (2006-2009): PLANETE is part of the IST UbiSec&Sen project. The goal of this project is to develop new security protocols for wireless sensor networks.

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'99-06, 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'05-06). 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. Thierry Turletti has served as an expert to the European Commission to evaluate and review EC funded projects.

Chadi Barakat organized the sampling 2005 workshop [1] in Paris together with Nick Duffield from AT&T on all aspects of internet traffic sampling, including statistical methodology and analysis, implementation in routers and collectors, and standardization. During 2005, Chadi Barakat also served on the Technical Program Committee of the following International Conferences and workshops: WONS 2006, WiNMee 2006, IMC 2005, and ICNP 2005. Chadi Barakat is guest editor for a JSAC special issue on sampling the Internet together with Jim Kurose from UMASS, Darryl Veitch from the University of Merlbourne and Gianluca Iannaccone from Intel Research Cambridge. The issue is

[1] http://adonis.lip6.fr/sampling/

expected to appear in Fall 2006. Chadi Barakat is also area editor for the ACM Computer Communication Review. During the year 2005, Chadi Barakat was invited to give keynotes at the E-next school on Modeling and Measuring the Internet in Louvain-La-Neuve in Belgium, at KTH in Stockholm, at the Asian School on Computer Sciences in Bangkok, and at ENSI in Tunis. Chadi Barakat is member of the recruitment committee at the computer science department of the University of Nice Sophia Antipolis, member of the directorial board for the Master RSD of the University of Nice, and responsible of the internship program at the latter Master.

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, which gathers most of the French academic research groups in networking area. 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. He also serves as an expert in RNRT commission on network protocols and architecture.

Arnaud Legout

- PC SIGCOMM'2006 (PC Light)
- Shadow PC SIGCOMM'2005
- Reviewer:
  - Journals: IEEE/ACM Transactions on Networking, IEEE/ACM Transactions on Computers, IEEE Network, Computer Communications.
  - Conferences: IEEE Infocom, ACM Sigmetrics.
- Organizer of 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).

Networks: Undergraduate course at ENSIMAG (Grenoble), by Vincent Roca

Mobile Networks: course at graduate studies program at Ensimag by 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

9.3. PhD Theses and Internships

9.3.1. PhD defended in 2005

1. Lina Al-Chaal defended his PhD on March 2005. The work has addressed several aspects of VPN (Virtual Private Network) like VPN and group communications, VPN and Web Services, redundant VPN techniques.
2. Christoph Neumann defended his PhD on December 2005; The work has addressed several aspects of group communication and FEC codes, including LDPC FEC, FLUTE extensions, and scalable video streaming.
3. Hossein Manshaei defended his PhD on December 2005; The work has addressed several aspects of Multimedia Communications Protocols with cross-layering optimization.
4. Vijay Arya defended his PhD on July 2005; The work has addressed several aspects of Multimedia transmission control algorithms for new generation mobile terminals.

9.3.2. Ongoing PhDs

1. Abdel Basset Trad works on “Adaptive VoIP Transmission over Heterogeneous Wired/Wireless Networks”.
2. Laurent Fazio works on “Secured Multicast Overlays”.
3. Mohamed Ali Kaafar works on“ Interactive Multimedia applications on peer-to-peer networks”.
4. Hahnsang Kim works on “Agile Authentication Mechanism for Inter-domain Handoffs”.
5. Zainab Khallouf works on “Multicast Security : the Operator’s point of view”.
6. Mohamed Malli works on “Internet topology Inference”.
7. Diego Dujovne works on “Monitoring WiFi Networks”.

9.3.3. Training activities

1. Mohamed Abid worked on the Study of Bluetooth Authentication combined to a AAA system. Duration of the stay: 4 months from from September 15th 2004 to January 15th, 2005. Prepared degree: Diplôme d’Ingénieur en Informatique. Affiliation: ENSI, Tunisia.
2. Maxime BAUDOT worked on Enhancing the Azureus software Duration of the stay: 2 months from June 27th to September 2nd, 2005. Prepared degree: Diplôme d’ingénieur Affiliation: ESSI - Sophia Antipolis
3. Vincent CHARPIN worked on an evaluation of the PlanetLab platform Duration of the stay: 3 months from April 11th to July 13th, 2005 Prepared degree: Diplôme d’ingénieur Affiliation:Ecole Polytechnique - France
4. Diego Roberto DUJOVNE worked on the design and implementation of a WIFI probe. Duration of the stay : 6 months from January 12th to July 12th 2005 Prepared degree: Master in Computer Science Affiliation: University of Cordoba - Argentine
5. Mohamed Chedly GHEDIRA worked on Multicast transmission of Multimedia flows over multiple wireless channels. Duration of the stay: 4 months from march 1st to June 24th, 2005. Prepared degree: Diplôme d’ingénieur Affiliation: Ecole Nationale des sciences de l’informatique - Tunisia
6. Wolf Heinrich LAUPPE worked on Multimedia transmission over multiple wireless channels Duration of the stay: 4 months from April 11th to August 15th, 2005 Prepared degree: Diplôme d’ingénieur Affiliation:Ecole Polytechnique - France

7. Farukh MUNIR worked on adaptive transmission of voice over IP in an 802.11E wireless LAN environment. Duration of the stay: 5 months from march 1st to August 31st, 2005. Prepared degree: Master STIC Spécialité RSD Affiliation:Universite Nice Sophia Antipolis
8. Hangartner Roman worked on the design and analysis of peer-to-peer protocols for multimedia applications. Duration of the stay: September 1st to February 28th, 2005 Prepared degree: EPFL Engineering Degree. Affiliation: EPFL, Switzerland.

10. Bibliography

Articles in refereed journals and book chapters

[1] I. AAD, Q. NI, C. BARAKAT, T. TURLETTI. *Enhancing IEEE 802.11 MAC in congested environments*, in "Elsevier Computer Communications Journal (Special Issue on ASWN 2004)", vol. 28, n^o 14, September 2005, p. 1605-1617.

[2] P. ANSEL, Q. NI, T. TURLETTI. *FHCF: An Efficient Scheduling Scheme for IEEE 802.11e*, in "to appear in ACM/Kluwer MONET, Special Issue devoted to WiOpt 2004".

[3] H. ASAEDA, V. ROCA. *Policy and scope management for multicast channel*, in "IEICE Transactions on Information and System, Vol. 88 No. 7", July 2005.

[4] C. BARAKAT, M. MALLI, N. NONAKA. *TICP: Transport Information Collection Protocol*, in "accepted for publication in Annals of Telecommunications".

[5] G. CANTIENI, Q. NI, C. BARAKAT, T. TURLETTI. *Performance Analysis of Finite Load Sources in 802.11b Multirate Environments*, in "Computer Communications Journal, Special issue on performance issues of WLANs, PANs, and Ad Hoc networks", vol. 28, n^o 10, June 2005, p. 1095-1109.

[6] C. CASTELLUCCIA, S. JARECKI, J. KIM, G. TSUDIK. *Secure Acknowledgment Aggregation*, in "Computer Networks (Elsevier), special issue on Networking Algorithms", december 2005.

[7] W. DABBOUS, T. TURLETTI. *Multicast Multimédia sur Internet, Traité Collection IC2, Série Réseaux et Télécoms*, A. BENSLIMANE (editor). , chap. Le Multipoint pour les Environnements Virtuels à Grande Échelle, HERMES Science Publications, March 2005.

[8] H. KIM, T. TURLETTI, A. BOUALI. *A Formal Toolkit for Developing DSP Software Applications*, in "Theory and Practice in Logic Programming", vol. 6 Issue 1, Feb. 2005, p. 1-31.

[9] M. MANSHAEI, T. TURLETTI, T. GUIONNET. *An Evaluation of Media-Oriented Rate Selection Algorithm for Multimedia Transmission in MANETs*, in "to appear in EURASIP Journal on Wireless Communications and Networking, Special Issue on Ad Hoc Networks: Cross-Layer Issues".

[10] C. NEUMANN, V. ROCA, R. WALSH. *Large scale content distribution protocols*, in "ACM Computer Communication Review (CCR), Vol 35 No. 5 (invited paper)", October 2005.

[11] Q. NI, T. LI, T. TURLETTI, Y. XIAO. *Saturation throughput analysis of error-prone 802.11 wireless networks*, in "Wireless Communications and Mobile Computing (WCMC)", vol. 5, n^o 8, December 2005, p. 945-956.

[12] Q. NI, T. TURLETTI. *Wireless LANs and Bluetooth*, Y. XIAO, Y. PAN (editors). , chap. QoS Support for IEEE 802.11 WLAN, Book chapter to appear in Nova Science Publishers.

[13] T. PLAGEMANN, V. GOEBEL, L. MATHY, T. TURLETTI, G. URVOY-KELLER. *From content distribution networks to content network-issues and challenges*, in "to appear in Computer Communications journal".

[14] V. ROCA. *chapitre 5: Fiabilité dans les communications de groupe : une introduction, and chapitre 6: Les approches de bout en bout de support de la fiabilité*, in "Multicast multimedia sur Internet book, Hermes, ISBN 2-7462-1063-0", 2005.

[15] T. TANSUPASIRI, K. KANCHANASUT, C. BARAKAT, P. JACQUET. *Using Active Networks Technology for Dynamic QoS*, in "accepted for publication in Computer Networks".

Publications in Conferences and Workshops

[16] E. ALTMAN, C. BARAKAT, V. RAMOS. *Analysis of AIMD protocols over paths with variable delay*, in "IEEE INFOCOM, Hong Kong", March 2004.

[17] V. ARYA, T. TURLETTI, T. FRIEDMAN, R. BELLINO, N. DUFFIELD. *Low Feedback MINC Loss Tomography*, in "Poster at Infocom Student Workshop, Miami, FL, USA", March 2005.

[18] V. ARYA, T. TURLETTI, C. HOFFMANN. *Feedback Verification for Trustworthy Tomography*, in "3rd Workshop on Internet Performance, Simulation, Monitoring and Measurement (IPS-MOME), Warsaw, Poland", March 2005.

[19] V. ARYA, T. TURLETTI, S. KALYANARAM. *Encodings of Multicast Trees*, in "IFIP Networking, Waterloo Ontario, Canada", May 2005.

[20] C. BARAKAT, G. IANNACCONE, C. DIOT. *Ranking flows from sampled traffic*, in "in proceedings of CoNEXT, Toulouse", Octobre 2005.

[21] T. BRAUN, V. ARYA, T. TURLETTI. *A Backup Tree Algorithm for Multicast Overlay Networks*, in "Poster at IFIP Networking, Waterloo Ontario, Canada", May 2005.

[22] T. BRAUN, H. KIM. *Efficient Authentication and Authorization of Mobile Users Based on Peer-to-Peer Network Mechanisms*, in "HICSS, Hawaii, U.S.A.", IEEE, Jan. 2005, 306b.

[23] C. CASTELLUCCIA, G. AVOINE. *Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags*, in "Proceedings of CARDIS 2006, Spain", march 2006.

[24] C. CASTELLUCCIA, P. MUTAF. *Shake Them Up!*, in "Proceedings of ACM/Usenix Mobisys 2005, Seattle, U.S.A.", ACM, june 2005.

[25] C. CASTELLUCCIA, E. MYKLETUN, G. TSUDIK. *Efficient Aggregation of Encrypted Data in Wireless Sensor Networks*, in "Proceedings of ACM Mobiquitous 2005, San Diego", ACM, july 2005.

[26] C. CASTELLUCCIA, N. SAXENA, J. YI. *Self-Configurable Key Pre-distribution in Mobile Ad-Hoc Networks*, in "Proceedings of IFIP Networking 2005, Ontaria, Canada", IFIP, May 2005.

[27] N. DUFFIELD, V. ARYA, R. BELLINO, T. FRIEDMAN, J. HOROWITZ, D. TOWSLEY, T. TURLETTI. *Network Tomography from Aggregate Loss Reports*, in "IFIP WG 7.3 International Symposium on Computer Performance, Modeling, Measurements and Evaluation (Performance'05), Juan-Les-Pins, France", October 2005.

[28] C. HOFFMANN, M. MANSHAEI, T. TURLETTI. *CLARA: Closed-Loop Adaptive Rate Allocation for IEEE 802.11 Wireless LANs*, in "IEEE WirelessCom'05, Hawai, USA", June 2005.

[29] Z. KHALLOUF, V. ROCA, R. MOIGNARD, S. LOYE. *A Filtering Approach for an IGMP Flooding Resilient Infrastructure*, in "4ème Conférence sur la Sécurité et Architectures Réseaux (SAR'05), Batz sur Mer, France", June 2005.

[30] H. KIM, W. DABBOUS, H. AFIFI. *A Bypassing Security Model for Anonymous Bluetooth Peers*, in "Wirelesscom, Hawaii, U.S.A.", vol. 1, IEEE, June 2005, p. 310-315.

[31] H. KIM, K. G. SHIN, W. DABBOUS. *Improving Cross-domain Authentication over Wireless Local Area Networks*, in "SecureComm, Athens, Greece", IEEE, Sep. 2005.

[32] M. LACAGE, M. MANSHAEI, T. TURLETTI. *A Practical Approach to Rate Adaptation*, in "ACM/IEEE MSWIM, Venice, Italy", October 2004.

[33] M. MALLI, C. BARAKAT, W. DABBOUS. *An Efficient Approach for Content Delivery in Overlay Networks*, in "in proceedings of IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas", January 2005.

[34] M. MALLI, C. BARAKAT, W. DABBOUS. *Application-level versus Network-level Proximity*, in "in proceedings of the Asian Internet Engineering Conference (AINTEC), Bangkok", December 2005.

[35] M. MANSHAEI, G. CANTIENI, C. BARAKAT, T. TURLETTI. *Performance Analysis of the IEEE 802.11 MAC and Physical Layer Protocol*, in "IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Taormina, Italy", June 2005.

[36] P. MUTAF, C. CASTELLUCCIA. *Compact Neighbour Discovery (a bandwidth defense through bandwidth optimization)*, in "Proceedings of IEEE INFOCOM 2005, Miami, U.S.A.", IEEE, March 2005.

[37] C. NEUMANN, V. ROCA, A. FRANCILLON, D. FURODET. *Impacts of Packet Scheduling and Packet Loss Distribution on FEC Performances: Observations and Recommendations*, in "ACM CoNEXT'05 Conference, Toulouse, France", October 2005.

[38] C. NEUMANN, V. ROCA. *Impacts of the Startup Behavior of Multilayered Multicast Congestion Control Protocols on the Performance of Content Delivery Protocols*, in "IEEE 10th International Workshop on Web Content Caching and Distribution, Sophia Antipolis, French Riviera, France, (also in INRIA Research Report RR-5578)", September 2005, http://www.inria.fr/rrrt/rr-5578.html.

[39] Q. NI, T. TURLETTI, Y. XIAO. *Performance Analysis of the IEEE 802.11e Block ACK Scheme in a Noisy Channel*, in "2nd International Conference on Broadband Networks, Boston, MA, USA", October 2005.

[40] A. TRAD, F. MUNIR, H. AFIFI. *Capacity Evaluation of VoIP in IEEE 802.11e WLAN Environment*, in "Proceedings of CCNC'06, Las Vegas, U.S.A.", IEEE, Jan. 2006.

Internal Reports

[41] S. FAURITE, A. FRANCILLON, V. ROCA. *TESLA source authentication in the ALC and NORM protocols*, IETF RMT Working Group, Work in Progress, July 2005.

[42] A. A. HAMRA, C. BARAKAT, T. TURLETTI. *Network Coding for Wireless Mesh Networks: A Case Study*, Technical Report, n^o inria-00000874 - version 1, INRIA, November 2005, http://hal.inria.fr/inria-00000874.

[43] M. A. KAAFAR, T. TURLETTI, W. DABBOUS. *Locate, Cluster and Conquer: A Scalable Topology-Aware Overlay Multicast*, Technical Report, n^o RT-0314, INRIA, November 2005, http://www.inria.fr/rrrt/rt-0314.html.

[44] J. LACAN, V. ROCA, J. PELTOTALO, S. PELTOTALO. *Reed Solomon error correction scheme*, IETF RMT Working Group, Work in Progress, October 2005.

[45] A. LEGOUT, G. URVOY-KELLER, P. MICHIARDI. *Understanding BitTorrent: An Experimental Perspective*, Technical Report, n^o inria-00000156, version 3 - 9 November 2005, INRIA, November 2005, http://hal.inria.fr/inria-00000156.

[46] T. LI, Q. NI, D. MALONE, D. LEITH, Y. XAO, T. TURLETTI. *A new MAC scheme for Very High-Speed WLANs*, Technical Report, n^o HI-2005-1101, Hamilton Institute, November 2005.

[47] C. NEUMANN, V. ROCA, J. LABOURÉ, Z. KHALLOUF. *An Open-Source LDPC/LDGM Large Block FEC Codec*, http://www.inrialpes.fr/planete/people/roca/mcl/.

[48] C. NEUMANN, V. ROCA, R. WALSH. *A file aggregation scheme for FLUTE*, IETF RMT Working Group, Work in Progress, October 2005.

[49] T. PARMENTELAT, A. GOURDON, T. TURLETTI, E. LARREUR. *A Very Large Virtual Environment for Multimedia Conferencing*, Technical Report, n^o 0296, INRIA, May 2004, http://www.inria.fr/rrrt/rt-0296.html.

[50] V. ROCA, C. NEUMANN, D. FURODET. *Low Density Parity Check (LDPC) Forward Error Correction*, IETF RMT Working Group, (WG Item), Work in Progress, October 2005.

[51] V. ROCA, C. NEUMANN. *Design, Evaluation and Comparison of Four Large Block FEC Codecs, LDPC, LDGM, LDGM Staircase and LDGM Triangle, plus a Reed-Solomon Small Block FEC Codec*, Research Report, n^o 5225, INRIA, June 2004, http://www.inria.fr/rrrt/rr-5225.html.

[52] V. ROCA, ET AL.. *MCLv3: an Open Source GNU/GPL Implementation of the ALC and NORM Reliable Multicast Protocols*, http://www.inrialpes.fr/planete/people/roca/mcl/.