INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team PLANÈTE

Protocoles et Applications pour l'Internet

Sophia Antipolis - Rhône-Alpes

THEME COM

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
Hitoshi Asaeda [Senior Engineer]
Alexis Gourdon [Expert Engineer]
Julien Labouré [Expert Engineer]
Pars Mutaf [Expert Engineer]
Christoph Neuman [Expert Engineer]
Thierry Parmentelat [Senior Engineer]
Ni Qiang [Expert Engineer to April 30th]

Post doc
Ceilidh Hoffmann [from September 1st]
Dongliang Guan [from November 1st]

PhD students
Lina Al-Chaal [Funding CIFRE, Netcelo]
Vijay Arya [Funding RNRT VIP]
Laurenţiu Barză [Funding RNRT VTHD++]
Ayman El-Sayed [Egyptian government scholarship]
Hossein Manshaei [Funding MESR]
Hahnsang Kim [Funding Hitachi contract]
Abdel Basset Trad [Funding RNRT VTHD++]
Laurent Fazio [Funding CIFRE, ST]
Zainab Khallouf [Funding CIFRE, FT R&D]
Mohamed Malli [Funding MESR]
Mohamed Ali Kaafar [Funding MUSE project]

Trainees
Mohamed Abid [ENSI, from march 15th to June 15th and from september 15th to January 15th, 2005]
Hangartner Roman [EPFL, from September 1st to February 28th, 2005]
Abdramane Diallo [DEA RSD, from march 1st to September 30th]
Tianji Li [DEA RSD, from march 1st to September 30th]
Danila Koudriashov [Ecole Polytechnique, from April 16th to July 16th]
Wacharapol Pokavanic [AIT, from September 15th to December 30th]
Musfiq Rahman [AIT, from September 15th to January 15th, 2005]

2. 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, 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.

Further, we apply techniques of the information and queuing theories to evaluate the performance of the studied problems.

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 infrastructureless 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** : Mobile Ad-Hoc networks and Wireless Sensor Networks are in fact highly networked environments that create many new exciting security and privacy challenges. We are interested in mainly in the design of new key exchange protocols and of secured routing protocols. We also work on location privacy techniques, authentication cryptographic protocols and opportunistic encryption. Our goals are to understand the security issues in those constrained networks environments 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 desgin 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. Successful interoperability tests with three other ALC/FLUTE implementations (Nokia, Univ. of Tempere, Univ. of Bremen) have been carried out in 2004. This work is done by V. Roca, C. Neumann (and J. Labouré till October 2003).

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 2004. This work is done essentially by C. Neumann, V. Roca, A. Francillon (and J. Labouré and Z. Khallouf till October 2003). See http://www.inrialpes.fr/planete/people/roca/mcl/ldpc_infos.html for more information.

5.3. 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.

5.4. 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 [52].

5.5. 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 protoype 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, Hahnsang Kim, Christoph Neuman, Pars Mutaf.

- **Robust Self-Keying Mobile Ad-Hoc Networks**
  We developped 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 litterature recently. Results clearly indicate that the new scheme is much more practical.

- **Crypto-less key exchange**
We developped 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 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.

- **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.

- **Secret handshake**
  Secret handshake protocols were recently introduced to allow members of the same group to authenticate each other *secretly*, in the sense that someone who is *not* a group member cannot tell, by engaging some party in the handshake protocol, whether that party is a member of this group. On the other hand, any two parties who *are* members of the same group will recognize each other as members. Thus, a secret handshake protocol can be used in any scenario where group members need to identify each other without revealing their group affiliations to outsiders.
  Previous work constructed a secret handshake protocol secure under the *Bilinear Diffie-Hellman* (BDH) assumption in the Random Oracle Model (ROM). We show how to build secret handshake protocols secure under more standard cryptographic assumptions, like *Computational Diffie Hellman* (CDH), using a novel tool of *CA-oblivious* public key encryption, which is an encryption scheme s.t. neither the public key nor the ciphertext reveal any information about the Certification Authority (CA) which certified the public key. We construct CA-oblivious encryptions and handshake schemes based (in ROM) on either the Computational Diffie-Hellman or the RSA assumption.

- **SSL server protection against DoS attacks**
  Much of today's distributed computing takes place in a client/server model. Despite advances in fault tolerance – in particular, replication and load distribution – server overload remains to be a major problem. In the Web context, one of the main overload factors is the direct consequence of expensive Public Key operations performed by servers as part of each SSL handshake. Since most SSL-enabled servers use RSA, the burden of performing many costly decryption operations can be very detrimental to server performance. This work examines a promising technique for re-balancing RSA-based client/server handshakes. This technique facilitates more favorable load distribution by requiring clients to perform more work (as part of encryption) and servers to perform commensurately less work, thus resulting in better SSL throughput. Proposed techniques are based on careful adaptation of variants of **Server-Aided RSA** originally constructed for smart cards. Experimental results demonstrate that suggested methods (termed **Client-Aided RSA**) can speed up processing by a factor of between 11 to 19, depending on the RSA key size. This represents a considerable improvement. Furthermore, proposed techniques can be a useful companion tool for SSL Client Puzzles in defense against DoS and DDoS attacks.

- **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.

- **IPv6 Opportunistic Encryption**
  The main idea of opportunistic encryption is to deploy security gateways that will sit between the border of intranets (private networks) and the Internet. A gateway intercepts an outgoing packet aimed at a remote host, and attempts to negotiate an IPsec tunnel to that host's security gateway. If the attempt succeeds, traffic can then be secured transparently (without changes to the end-host software). If the attempt fails, packets are sent through in the clear or dropped, according to the local policy. Opportunistic encryption allows secure (encrypted, authenticated) communication via IPsec without connection-by-connection pair-wise pre-arrangement.
  Our 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.
- **IPv6 Crypto. Generated Addresses (CGA) for Constrained Devices**
  Cryptographically Generated Addresses (CGAs) have been designed to solve the so-called IPv6 *Address Ownership* problem. The current IETF CGA proposal relies on RSA signature. Generating an RSA signature is quite expensive and might be prohibitive for small devices with limited capacities. For example, a 1024-RSA signature requires approximately 1536 modular multiplications.
  In this work, we proposed a new CGA scheme whose verification requires fewer than 10 modular multiplications. We achieve this performance gain by (1) selecting an efficient signature scheme, namely the small prime variation of the Feige-Fiat-Shamir scheme and (2) tuning the cryptographic parameters of this signature scheme to the security strength of the CGA (i.e. the size of the hash function used to generate it).
- **Efficient Authentication for Fast Inter-domain Handoffs**
  Last year, we proposed a hierarchical authentication architecture by presenting 'brokers' playing a role of an auxiliary server in the authentication mechanism. It led to a subsequent interest about where to locate the broker to minimize the authentication latency as the mobile node moves along. We have also presented a mathematical method to help optimizing the architecture.
  On top of the optimized authentication architecture, we proposed this year a mutual authentication and key distribution protocol. This protocol supports a secure fast inter-domain handoffs with two different modes: the initial mode and reiteration mode. In the initial mode, it completes the authentication and key distribution procedure in the 4-way handshake. It, in turn, generates a security context, in which security information is included. Afterwards, in the reiteration mode, re-authentication is compactly performed in the 2-way handshake. We work also on how to improve secure fast inter-domain handoffs with a security contexts pre-caching mechanism.

6.2. Scalable Group Communications

Participants: Vijay Arya, Lina AlChaal, Laurentiu Barza, Walid Dabbous, Alexis Gourdon, Christoph Neuman, Thierry Parmentelat, Vincent Roca, Ayman El-Sayed, Thierry Turletti.

- **Reliable multicast protocols** We actively participate to the RMT working group at the IETF, and in particular work on FLUTE (File Delivery over Unidirectional Transport) in the IETF RMT working group. FLUTE is now standardized as RFC 3926, 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.

Several extensions are currently being considered to FLUTE: a file aggregation scheme for FLUTE (INRIA-Nokia Internet-Draft); Reed-Solomon and Parity Check Matrix-based FEC schemes for FLUTE and similar protocols (Univ. of Tempere-INRIA Internet-Draft); FLUTE Interoperabtility Testing Guidelines (Nokia-INRIA-Univ. of Tempere Internet-Draft).
We also contribute to the ALC, LCT, FEC information, FEC building block, and NORM building block RFC's by providing comments and suggestions. We also developed one of the reference implementations of the ALC/LCT and FLUTE standards. This implementation is widely known and is used by several groups, including in commercial applications. File delivery over satellite, in 3GPP or DVB environments is one of its major fields of application.

- **Scalable Video Streaming over ALC**
  SVSoA is a novative solution for the large scale streaming of video contents. It provides many advantages over more traditional approaches : massive scalability, TCP friendliness, high robustness in front of loss bursts, no QoS requirement (or other dedicated services) within the core network, and compatibility with any video encoding schemeq.
  Two variants have been designed and evaluated: version 1 (2003) was focussing Internet-wide transmissions, while version 2 (2004) is more focussed on robust wireless transmissions. A prototype has been developped, that takes advantage of our work on ALC/LCT and MCLv3. This activity was supported by STmicroelectronics in 2004.

- **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 [55]. Our work in this domain has focused on serveral 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. A large amount of work remains to be done on this promising class of FEC codes, in particular concerning their use in various environments [37].
  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. We know several operational uses by private companies. In particular, this work has been largely supported by STmicroelectronics in 2004.

- **Application Level Multicast**
  Multicast routing is not as widely deployed as could have been expected, and offering alternative group communication services has become a very active field of research. In this work we have designed and evaluated such a service, which creates and manages an overlay on which packets can be distributed to several concurrent receivers. We have also analyzed how cheating can easilly defeat the system, which means that new security and incentive-based solutions are needed, not only in our proposal, but more generally to most application level multicast solutions [11].

- **Scalable Communication Protocols for Large Scale Virtual Environments**
  We have designed a new communication layer which is suitable for real-time multimedia virtual environments (VEs) that need to achieve high scalability such as computer games involving multimedia exchanges. Our mechanism is located at the transport-layer, using multiple multicast groups and multiple agents. It involves the dynamic partitioning of the virtual environment into spatial areas and the association of these areas with multicast groups. Our first approach called SCORE was

based on the Any Source Multicast (ASM) model [10]. It uses a method based on the theory of planar point processes to determine an appropriate cell-size, so that the incoming traffic at the receiver side remains with a given probability below a sufficiently low threshold. Our second approach called SCORE-SSM is based on the Single Source Multicast (SSM) model as the underlying network infrastructure. Though the SSM model might, at first glance, look more appropriate for streaming-like applications, we show that it is possible to take advantage of such a communication layer to solve the new issues that the application layer has to address in the SSM environment. We even outline that SSM has benefits over Any Source Multicast (ASM), in that it provides greater flexibility in flow management. As opposed to alternative techniques such as peer-to-peer overlays, the use of network-layer multicast performs very well in terms of latency. Our demonstration application embeds multimedia conferencing capabilities to demonstrate that real-time and massively multi-player applications can be successfully implemented on top of this communication layer [51].

- **Encodings of Multicast Trees**
  We have also 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 [42].

- **Explicit Routing in 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 [44].

- **VPN-based Web Services**
  In this work, We showed how to build a fully secure and efficient group communication service between several sites. This service is built on top of a VPN environment where IPSec tunnels are created, on-demand, between the various sites that need to communicate. The proposed approach is innovative and departs from the more traditional “provider provisioned” VPN solution where the same entity, namely the ISP, needs to master both the infrastructure and the VPN management. Although this approach simplifies many aspects, it requires the same ISP to manage all sites, which is too restrictive.
  Web Services offer standardized and easy communications for distributed systems over the Internet. However their dynamic and distributed nature requires a well-managed system, and pending security issues prevent their widespread adoption. Meanwhile there is a big rage toward the use of Virtual Private Networks (VPNs) to secure communications over the Internet. In this work we explain how to merge these two technologies in a new powerful hybrid model that: (1) enables an easy management of web services, (2) provides web services security thanks to the use of dynamic and programmable VPNs, and (3) remains simple and fully integrated.

6.3. Impact of Heterogeneity on Protocol Performance

Participants: Imad Aad, Pierre Ansel, Vijay Arya, Chadi Barakat, Gion-Reto Cantieni, Mathieu Lacage, Mohammad Malli, Hossein Manshaei, Qiang Ni, Thierry Turletti.

- **Congestion Control for Multicast layered Video Transmission** We have designed a new congestion control algorithm called Source-channel Adaptive Rate Control (SARC) for layered video transmission in large multicast groups. In order to solve the well-known feedback implosion problem in large multicast groups, we have implemented a mechanism for filtering *RTCP* receiver reports sent from receivers to the whole session. The proposed filtering mechanism provides a classification of receivers according to a predefined similarity measure. SARC includes an end-to-end source and FEC rate control based on this distributed feedback aggregation mechanism coupled with a video layered coding system. The number of layers, their rate and levels of protection are adapted dynamically to aggregated feedbacks [17].
- **Misbehavior Detection in Multicast Inference of Network Characteristics**
  Network tomography tools such as MINC (Multicast Inference of Network Characteristics) can be used to infer important internal properties of a network underlying a multicast tree. This inference is made by analyzing receiver feedbacks to the measurement probes sent from the source and can be utilized to make significant decisions concerning the network. However, 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 [41].
- **Large Scale VoIP transmission over Heterogeneous Network Environement**
  We have proposed in [40] an adaptive architecture for the transport of VoIP traffic over heterogeneous wired/wireless Internet environments. This architecture uses a VoIP gateway associated with an 802.11e QoS enhanced access point (QAP) to transcode voice flows before their transmissions over the wireless channel. The instantaneous bit rate is determined by a control mechanism based on the estimation of channel congestion state. Our mechanism dynamically adapts audio codec bit rate using a congestion avoidance technique so as to preserve acceptable levels of quality. A case study presenting the results relative to an adaptive system transmitting at bit rates typical of G.711 PCM (64 kbit/s) and G.726 ADPCM (40, 32, 24 and 16 kbit/s) speech coding standards illustrates the performance of the proposed framework. We perform extensive simulations to compare the performance between our adaptive audio rate control and TFRC mechanism. The results show that the proposed mechanism achieves better voice transmission performance, especially when the number of stations is fairly large.
  Currently, we are developing a SIP-based hybrid peer-to-peer architecture for VoIP networks that uses IP path selection. In this work, we propose a novel hybrid peer-to-peer architecture that is based on the joint use of SIP primitives and Internet “path quality” measurements, such as delay, loss rate and jitter in order to select the “best quality” IP path for a long distance voice communication (e.g., international call). We motivate our approach by the existence of better quality alternative path due to the heterogeneity of current Internet environements. We show significant delay and loss rate improvement over IP telephony strategies currently used in the Internet.
- **IEEE 802.11 Performance Improvements**
  Automatic rate adaptation in IEEE 802.11 WLANs may cause drastic throughput degradation for high speed bit rate stations. The CSMA/CA medium access method guarantees equal long-term channel access probability to all hosts when they are saturated. Recent works have shown that the saturation throughput of any station is limited by the saturation throughput of the station with the

lowest bit rate in the same infrastructure. In order to overcome this problem, we have designed a new model for finite load sources with multirate capabilities. We have used this model to investigate the throughput degradation outside and inside the saturation regime. We have defined a new fairness index based on the channel occupation time to have more suitable definition of fairness in multirate environments. Further, we have proposed two simple but powerful mechanisms to partly bypass the observed decline in performance and meet the proposed fairness. The model for finite load sources can also be used to evaluate our proposed mechanisms in terms of total throughput and MAC layer delay for various network configurations [7].
We have also study how to enhance IEEE 802.11 MAC in congested environments. In the DCF access scheme, contention windows (CW) change dynamically to adapt to the contention level: Upon each collision, a node doubles its CW to reduce further collision risks. Upon a successful transmission, the CW is reset, assuming that the contention level has dropped. However, contention level is more likely to change slowly, and resetting the CW causes new collisions and retransmissions before reaching the optimal value again. This wastes bandwidth and increases delays. We have analyzed simple slow CW decrease functions and compare their performances to the legacy standard. Simulations and mathematical modeling show that slow decrease functions increase the performance at all contention levels and transient phases, especially in high congested environments [18].
In parallel, we have studied mechanisms to efficiently select physical rate transmission in IEEE 802.11 WLANs. Today, three different physical (PHY) layers for the IEEE 802.11 WLAN are available (802.11a/b/g); they all provide multi-rate capabilities. To achieve high performance under varying conditions, these devices need to adapt their transmission rate dynamically. While this rate adaptation algorithm is a critical component of their performance, only very few algorithms such as Auto Rate Fallback (ARF) or Receiver Based Auto Rate (RBAR) have been published and the implementation challenges associated with these mechanisms have never been publicly discussed. We have proposed an Adaptive ARF (AARF) algorithm for low latency systems that improves upon ARF to provide both short-term and long-term adaptation. The new algorithm has very low complexity while obtaining a performance similar to RBAR, which requires incompatible changes to the 802.11 MAC and PHY protocol. We have also designed a new rate adaptation algorithm for high latency systems that has been implemented and evaluated on an AR5212-based device. Experimentation results show a clear performance improvement over the algorithm previously implemented in the AR5212 driver we used [46][34].
Finally, we have studied how to improve the effective throughput for transporting loss-tolerant multimedia traffic over a WLAN by taking into account both the application characteristics and the physical channel conditions. On this purpose, we have designed a media-oriented mechanism for selecting the appropriate transmission mode in 802.11-based wireless LANs (WLANs). In particular, the proposed cross-layer mechanism exploits the robustness of multimedia coding by allowing packets with corrupted payloads reach the receiving application. The sending application specifies its quality of service requirements (data rate, BER tolerance, etc.), and the receiver selects the best transmission mode (transmission rate, modulation scheme, FEC scheme) while taking into account the time-varying channel conditions. The results indicate that the proposed cross-layer approach achieves up to 5 Mbps increase in throughput and 20-meter increase in the coverage range. Furthermore, by disabling FEC from some of the standard transmission modes, we show that the goodput of loss-tolerant applications can be improved significantly [36].

- **QoS Support for IEEE 802.11e WLANs**
  The emerging widespread use of real-time multimedia applications over wireless networks makes the support of Quality of Service (QoS) a key problem. The IEEE 802.11e Medium Access Control (MAC) is an emerging standard to support Quality of Service (QoS) [15].
  We have designed a new scheme called *adaptive fair EDCF* that extends EDCF, by increasing the contention window during deferring periods when the channel is busy, and by using an adaptive fast

backoff mechanism when the channel is idle. Our scheme computes an adaptive backoff threshold for each priority level by taking into account the channel load. The new scheme significantly improves the quality of multimedia applications. Moreover, it increases the overall throughput obtained both in medium and high load cases. Simulation results show that our new scheme outperforms EDCF and other enhanced schemes [35].
Some recent works show that the IEEE 802.11e Hybrid Coordination Function (HCF) can improve significantly the QoS support. A simple HCF scheduler has been proposed in the 802.11e which takes the QoS requirements of flows into account and allocates time to stations on the basis of the mean sending rate. We have shown that this HCF scheduling algorithm is only efficient for flows with strict Constant Bit Rate (CBR) characteristics. However, a lot of real-time applications, such as videoconferencing, have small variations in their packet sizes, sending rates or even have Variable Bit Rate (VBR) characteristics. We have designed a new HCF scheduling algorithm, FHCF, that aims to be fair for both CBR and VBR flows. The FHCF scheme uses queue length estimations to tune its time allocation to stations. Our performance study indicates that FHCF provides good fairness while supporting bandwidth and delay requirements for a large range of network loads [22].

- **TCP over high speed links**
  The TCP protocol carries most of Internet traffic and is of major importance for the stability of the Internet. Understanding the performance of this protocol over the new transmission media that add to the Internet is a key point in deciding on how to adapt the TCP protocol to make it fully profit from the available resources in these media. We continued our analysis of TCP. Different transmission media were considered. Next is a summary of the results. Proposals to improve the performance of TCP in high speed networks have been recently put forward. Examples of such proposals include High-Speed TCP, Scalable TCP, and FAST TCP. In contrast to the additive increase multiplicative decrease algorithm used in the standard TCP, Scalable TCP uses a multiplicative increase multiplicative decrease (MIMD) algorithm for the window size evolution. In this work, we present a mathematical analysis of the MIMD congestion control algorithm in the presence of random losses. Random losses are typical to wireless networks but can also be used to model losses in wireline networks with a high bandwidth delay product. Our approach is based on showing that the logarithm of the window size evolution has the same behaviour as the workload process in a standard G/G/1 queue. The Laplace-Stieltjes transform of the equivalent queue is then shown to directly provide the throughput of the congestion control algorithm and the higher moments of the window size. Using *ns-2* simulations, we validate our findings using Scalable TCP which is an example of MIMD congestion control. The results can be found in [5].
- **TCP over variable delay links**
  The throughput of AIMD protocols in general and of TCP in particular, has been computed in many existing works by modeling the round-trip time as a constant and thus replacing it by its expectation. There are however many scenarios in which the delays of packets vary, causing a variation of the round-trip time. Many typical scenarios occur in wireless and mobile networks. We propose in this work an analytical model that accounts for the variability of delay, while computing the throughput of an AIMD protocol. We derive a closed-form expression for the throughput, that illustrates the impact of delay variability. We show by analysis and simulation, that an increase in the variability of delay improves the performance of an AIMD protocol. Thus, an analytical model that only considers the average delay could underestimate the performance of an AIMD protocol in scenarios where delay is variable. Our results appear in [21].
- **TCP over asymmetric links**
  The TCP congestion control protocol is mainly designed for bandwidth symmetric paths. As two-way asymmetric connections will probably become common case in the future with the widespread use of ADSL, satellites and other high-speed technologies, it is important to make sure that congestion will be properly handled in these environments. To this end, we propose in this work

a new Adaptive Class-based Queuing mechanism called ACQ for handling two-way TCP traffic over links that exhibit bandwidth asymmetry. ACQ runs at the entry of the slow link and relies on two separate classes, one for ACK packets and one for Data packets. ACQ proposes to adapt the weights of both classes according to the crossing traffic in order to maximize some utility function defined by the user or the network operator. We show by simulations that our mechanism is able to reach a good utilization of the available resources, managing then to maximize the satisfaction of the user of such asymmetric connections. More details to be found in [31].

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 dimensioning of its resources. In the monitoring part, we worked on new measurement techniques that scale with the fast increase in Internet traffic. We also worked on the utilization of measurements to infer the topology of the Internet and to localize any distributed resource. In the networking dimensioning part, we focused on a proper dimensioning of the Internet that improves the quality of service to users and that maximizes the operators revenue. Next is a sketch of our contributions in this area.

- **Traffic measurement**:
  Chadi Barakat visited Intel Research Cambridge to work on traffic measurement issues within the CoMo project. The visit was for six months starting from March 1st 2004. The main focus of the work was on how to sample packets in a core network so as to reduce the error in inverting the information about flows. Inverting flow properties using sampled traffic is known to be complex error prone procedure. The focus in the literature has been mainly on inverting some general properties of flows as the flow size distribution, the average flow size, or the total number of flows. We focused during this visit on the inversion of the properties of some specific flows and we considered as a metric the detection/ranking of top flows. We studied how efficient is this operation as a function of the sampling rate. Our results indicate that a high sampling rate is usually needed for the detection/ranking to be efficient, except if we limit ourselves to the top one or two flows, or if millions of flows are available. The study is done using probabilistic tools and trace-driven simulations. Preliminary results about this work can be found in [43].
- **Internet Topology Inference**:
  Internet operators and users are more and more interested in having an idea on the topology of the Internet and on the connectivity between the different networks and autonomous systems that compose it. The information on the topology serves for many purposes. For a network operator, this information allows to optimize the management of his network and the connectivity with the networks of other operators. For an Internet service provider, for example a provider of a content distribution network (CDN) service or a video on demand service, the information on the topology allows to optimize the placement of the servers and the management of the content to be distributed to users. The information on the topology is also necessary to optimize the routing at the overlay level. For an Internet end user, knowing the topology is important for the choice of the best ISP to connect to the Internet and for the optimization of end-to-end protocols as the protocols of lookup in peer-to-peer networks and the protocols of choice of the best servers from a set of replicated servers providing the same service.
  It is on this latter application of optimal server selection that we started our activity in the Planète group on the Internet topology inference. We came up with an enhanced model for the paths in the Internet, and based on this model, we proposed a scheme that allows an optimal choice of the best server among a set of replicated servers holding the same digital content to download. Our main objective is to reduce the content transfer time, which we define as the time required to download a digital content by a client using TCP. Our scheme consists of ranking the servers from the best

one to the worst one based on a metric that corresponds to a prediction of the content transfer time from each server. The prediction function considers the critical performance parameters that have an impact on the quality of the transfer, such as the load of the servers and the characteristics of the path between the client and the servers. Once the servers are ranked, the client can download the content on point-to-point from the best server, or in parallel from a subset of servers at the top of the list (best servers). Our experimental results show that our approach for identifying the best server(s) outperforms the existing classical solutions. The details about the proposed scheme and its validation with experimental results are published in CCNC 2005.

- **Two service classes for a better networking dimensioning**
  We study an approach to Quality of Service that offers end-users the choice between two service classes defined according to their level of transmission protection. The Fully Protected (FP) class offers end-users a guarantee of survivability in the case of a single link failure; all FP traffic is protected using a 1:1 protection scheme at the WDM layer. The Best-Effort Protected (BEP) class is not protected; instead restoration at the IP layer is provided. The FP service class mimics what Internet users receive today. The BEP traffic is designed to run over the large amounts of unused bandwidth that exist in today's Internet. The goal is to increase the load carried on backbone networks without reducing the QoS received by existing customers. To support two such services, we have to solve two problems: the off-line problem of mapping logical links to pairs of disjoint fiber paths, and an on-line scheduling problem for differentiating packets from two classes at the IP layer. We provide an algorithm based on a Tabu Search meta-heuristic to solve the mapping problem, and a simple but efficient scheduler based on Weighted Fair Queuing for service differentiation at the IP layer. We consider numerous requirements that carriers face and illustrate the tradeoffs they induce. We demonstrate that we can successfully increase the total network load by a factor between three and ten and still meet all the carrier requirements. The results of this work appeared in [16].

7. Contracts and Grants with Industry

7.1. Industrial contracts

Hitachi There is ongoing collaboration on security in Mobile Ad-Hoc Networks. The activity is described in the Security in Mobile Ad-Hoc networks section hereabove.

Alcatel We worked with Alcatel on Internet Topology inference described hereabove.

ST Microelectronics, Advanced Systems (AST), Grenoble : a 3 year contract has been set up (2002-2004) between INRIA/Planète and STM. Within this framework several tasks have been performed, each of them covered by a dedicated amendment to the contract: in 2002-2004, the development of a RoHC (Robust Header Compression) prototype; In 2003-2004, the improvement and analysis of an LDPC codec. In 2004, the development of a scalable video streaming prototype (SVSoA).

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).

Netcelo S.A., Grenoble a 3 year contract has been set up (November 2001 to October 2004) between INRIA/Planète and Netcelo S.A. for Lina Alchaal's PhD (CIFRE).

France Telecom R&D, Lannion a 3 year contract has been set up (2003-2005) between INRIA/Planète and FT R&D for Zainab Khallouf's PhD (CIFRE).

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.

VIP RNRT project (Oct 01 - Dec 04):
Video over Wireless IP. The aim of this project is to optimize quality of videoconferencing applications over wireless IP networks. Total amount is 88 Keuros. Extension until end of 2004.

VTHD++ RNRT project (Jan 02 - Dec 04):
follow-up of VTHD RNRT project was extended until end of 2004.

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

Chadi Barakat is:

- General chair of PAM 2004.
- Workshop chair in WiOpt'05.
- Technical Program Committee of GI&NGN symposium at Globecom 2004, PAM 2004, INFOCOM 2004, ASIAN 2002, ICNP 2002.
- Session chair in WiOpt 2003, ICNP 2002.
- Organizer of Mistral seminars (1999-2001), Planète seminars (2003-), and "séminaire croisé Réseau" (October 2003).

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 schoolds, 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.

9.2. University Techning

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 (12h), H. Afifi (12h).

Traffic Measurements: Optional course at the same program (24h), University of Nice-Sophia Antipolis, by C. Barakat.

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).

9.3. PhD Theses and Internships

9.3.1. PhD defended in 2004

1. Pars Mutaf defended his PhD on January 2004. The topic is Mobility management in all-IP networks.
2. Fatma Louati defended his PhD on February 2004. The topic is Asymetry and Bidirectional trafics on the Internet.
3. Ayman El-Sayed defended his PhD on March 2004. The topic is the design and evaluation of an application-level multicast protocol.
4. Laurentiu Barza defended his PhD on July 2004. The topic is Communication architecture for Large Scale Virtual Environments.

9.3.2. Ongoing PhDs

1. Vijay Arya works on “Multimedia transmission control algorithms for new generation mobile terminals”.
2. Abdel Basset Trad works on “Adaptive VoIP Transmission over Heterogeneous Wired/Wireless Networks”.
3. Lina Al-Chaal works on “Solutions for Multicast Security”.
4. Hossein Manshaei works on “Multimedia Communications Protocols with cross-layering optimization”.
5. Laurent Fazio works on “Secured Multicast Overlays".
6. Mohamed Ali Kaafar works on “Interactive Multimedia applications on peer-to-peer networks”.
7. Hahnsang Kim works on “Agile Authentication Mechanism for Inter-domain Handoffs”.
8. Zainab Khallouf works on “Multicast Security : the Operator’s point of view”.
9. Mohamed Malli works on “Internet topology Inference”.

9.3.3. Training activities

1. Mohamed Abid worked on the Study of Bluetooth Authentication combined to a AAA system. Duration of the stay: 7 months from march 15th to June 15th 2004 and from september 15th 2004 to January 15th, 2005. Prepared degree: Diplôme d’Ingénieur en Informatique. Affiliation: ENSI, Tunisia.
2. 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.
3. Tianji Li worked on the Optimization of the MAC layer protocols for IEEE 802.11n HSLANs. Duration of the stay: 1 March 2004 - 30th September 2004. Prepared degree: Master Réseaux et Systèmes Distribués. Affiliation: Sophia Antipolis, France.
4. Abdramane Diallo worked on the Congestion control for Large scale virtual environments. Duration of the stay: 1 March 2004 - 1st September 2004. Prepared degree: Master Réseaux et Systèmes Distribués. Affiliation: Sophia Antipolis, France.
5. Danila Koudriashov worked on the design and implementation of an application level multicast protocol in peer-to-peer networks. Duration of the stay: April 16th 2004 - July 16th 2004. Prepared degree: Ingénieur de l’Eecole Polytechnique. Affiliation: Ecole Polytechnique, France.
6. Wacharapol Pokavanic worked on the Implementation of a Channel Reflector. Duration of the stay : from September 15th to December 30th. Prepared degree : PhD at AIT.
7. Musfiq Rahman worked on the Developement of a Group Member authentication protocol for Ad-Hoc Networks. Duration of the stay : from September 15th to January 15th. Prepared degree : MSc at AIT.

10. Bibliography

Doctoral dissertations and Habilitation theses

[1] L. BARZA. *Communication architecture for Large Scale Virtual Environments*, Ph. D. Thesis, Université de Nice Sophia Antipolis, 2004.

[2] A. EL-SAYED. *Application Level Multicast Transmission Techniques over the Internet*, Ph. D. Thesis, INPG, 2004.

[3] F. LOUATI. *Asymetry and Bidirectional trafics on the Internet*, Ph. D. Thesis, Université de Nice Sophia Antipolis, 2004.

[4] P. MUTAF. *Signaling Optimizations for Neighbor Discovery, Paging and Mobility management in IPv6*, Ph. D. Thesis, INPG, 2004.

Articles in referred journals and book chapters

[5] E. ALTMAN, K. AVRACHENKOV, C. BARAKAT, A.-A. KHERANI, B. PRABHU. *Analysis of MIMD Congestion Control Algorithm for High Speed Networks*, in "Computer Networks Journal", 2004.

[6] F. F. G. ANIBA, W. DABBOUS. *Efficient Support of IP Multicast in the Next-Generation of GEO Satellite*, in "IEEE JSAC Special Issue on Broadband IP Networks via Satellites", 2004.

[7] G. CANTIENI, Q. NI, C. BARAKAT, T. TURLETTI. *Performance Analysis under Finite Load and Improvements for Multirate 802.11*, in "Special issue of Elsevier Computer Communications journal", December 2004.

[8] C. CASTELLUCCIA. *Cryptographically Generated Addresses for Constrained Devices*, in "Kluwer Wireless Personal Communications special issue on Wireless Security for Next Generation Communications", 2004.

[9] W. DABBOUS, T. TURLETTI. *Le multipoint pour les environnements virtuels à grande échelle*, chap. 11, Hermes Science Publication, 2004.

[10] E. LÉTY, T. TURLETTI, F. BACCELLI. *SCORE : a Scalable Communication Protocol for Large-Scale Virtual Environments*, in "IEEE/ACM Transactions on Networking", April 2004.

[11] L. MATHY, N. BLUNDELL, V. ROCA, A. EL-SAYED. *On Cheats in Application-Level Multicast*, in "IEEE INFOCOM'04", March 2004.

[12] G. MONTENEGRO, C. CASTELLUCCIA. *Crytographically-Based Identifiers (CBID): Concepts and Applications*, in "ACM Transaction on Information and System Security (TISSEC)", February 2004.

[13] P. MUTAF, C. CASTELLUCCIA. *Hash-based paging and location update using Bloom filters*, in "ACM/Kluwer Journal on Mobile Networks and Applications (MONET)", 2004.

[14] P. MUTAF, C. CASTELLUCCIA. *Hash-based paging and location update using Bloom filters*, in "ACM/Kluwer Journal on Mobile Networks and Applications (MONET)", vol. 10, n° 2, 2004.

[15] Q. NI, L. ROMDHANI, T. TURLETTI. *A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN*, in "Wireless Communication and Mobile Computing (WCMC)", vol. 4, n° 5, August 2004, p. 547-566.

[16] A. NUCCI, N. TAFT, C. BARAKAT, P. THIRAN. *Controlled Use of Excess Backbone Bandwidth for Providing New Services in IP-over-WDM Networks*, in "IEEE Journal on Selected Areas in Communications", vol. 22, n° 9, November 2004, p. 1692-1707.

[17] J. VIERON, T. TURLETTI, K. SALAMATIAN, C. GUILLEMOT. *Source and channel adaptive rate control for multicast layered video transmission based on a clustering algorithm*, in "EURASIP Journal on Applied Signal Processing (JASP)", February 2004.

Publications in Conferences and Workshops

[18] I. AAD, Q. NI, C. BARAKAT, T. TURLETTI. *Enhancing IEEE 802.11 MAC in congested environments*, in "4th IEEE Workshop on Applications and Services in Wireless Networks (ASWN), Boston, MA, USA", August 2004.

[19] L. ALCHAAL, V. ROCA, M. HABERT. *De l'Utilisation des VPNs pour l'Administration et la Sécurité des Services Web*, in "3ème Conférence sur la Sécurité et Architectures Réseaux (SAR'04), La Londe, France", June 2004.

[20] L. ALCHAAL, V. ROCA, M. HABERT. *Managing and Securing Web Services with VPNs*, in "2nd IEEE International Conference on Web Services (ICWS 2004)", July 2004.

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

[22] P. ANSEL, Q. NI, T. TURLETTI. *An Efficient Scheduling Scheme for IEEE 802.11e*, in "IEEE Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks Workshop (WiOpt), University of Cambridge, UK", March 2004.

[23] H. ASAEDA, W. DABBOUS. *Multicast Routers Cooperating with Channel Announcement System*, in "Proceedings of SAINT 2004 Workshops, Tokyo - Japan", january 2004.

[24] C. CASTELLUCCIA, F. DUPONT, G. MONTENEGRO. *A Simple Privacy Extension to Mobile IPv6*, in "IEEE/IFIP International Conference on Mobile and Wireless Communication Networks (MWCN), Paris", October 2004.

[25] C. CASTELLUCCIA, S. JARECKI, G. TSUDIK. *Secret-handshake from CA-Oblivious Encryption*, in "IACR ASIACRYPT, Korea", December 2004.

[26] C. CASTELLUCCIA, S. JARECKI, G. TSUDIK. *Secret-handshake from CA-Oblivious Encryption (short paper)*, in "ACM Symposium on Principles of Distributed Computing (PODC), Canada", July 2004.

[27] C. CASTELLUCCIA, S. JARECKI, G. TSUDIK. *Verifiable and Secure Acknowledgement Aggregation*, in "Fourth Conference on Security in Communication Networks '04 (SCN), Amalfi", September 2004.

[28] C. CASTELLUCCIA, G. MONTENEGRO, J. LAGANIER, C. NEUMAN. *Hindering Eavesdropping via IPv6 Opportunistic Encryption*, in "9th European Symposium on Research in Computer Security (ESORICS), Sophia-Antipolis", September 2004.

[29] C. CASTELLUCCIA, P. MUTAF. *Hash-based Dynamic Source Routing*, in "Networking 2004, Athens", May 2004.

[30] A. EL-SAYED, V. ROCA. *On Robustness in Application-Level Multicast: the Case of HBM*, in "9th IEEE Symposium on Computers and Communications (ISCC'04), Alexandria, Egypt", June 2004.

[31] W. D. FATMA LOUATI. *Adaptive Class-based Queuing for handling Two-Way traffic in Asymmetric Networks*, in "proceedings of the conference on High Speed Networks and Multimedia Communications (HSNMC), Toulouse", July 2004.

[32] Z. KHALLOUF, V. ROCA, R. MOIGNARD, S. LOYE. *Infrastructure Sécurisée de Routage Multipoint : le Point de Vue de l'Opérateur de Réseau*, in "3ème Conférence sur la Sécurité et Architectures Réseaux (SAR'04), La Londe, France", June 2004.

[33] H. KIM, H. AFIFI. *Automation of PIN Set-up for Bluetooth Security in Inter-Wireless Technology*, in "IEEE NOMS, Seoul", April 2004.

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

[35] M. MALLI, Q. NI, T. TURLETTI, C. BARAKAT. *Adaptive Fair Channel Allocation for QoS Enhancement in IEEE 802.11 Wireless LANs*, in "IEEE International Conference on Communications (ICC), Paris, France", June 2004.

[36] M. MANSHAEI, T. TURLETTI, M. KRUNZ. *Media-Oriented Transmission Mode Selection in 802.11 Wireless LAN*, in "IEEE WCNC, Atlanta, Georgia, USA", March 2004.

[37] C. NEUMANN, V. ROCA. *Analysis of FEC Codes for Partially Reliable Media Broadcasting Schemes*, in "2nd International Workshop on Multimedia Interactive Protocols and Systems (MIPS'04), Grenoble, France", November 2004.

[38] C. NEUMANN, V. ROCA. *Scalable Video Streaming over ALC (SVSoA): a Solution for the Large Scale Multicast Streaming of Videos*, in "First International Workshop on 'Streaming Media Distribution over the Internet' (SMDI04), Athens, Greece", May 2004.

[39] A. TRAD, H. AFIFI. *TFMC: a TCP-Friendly Multiplexing Control Scheme for VoIP Flow Transmission*, in "ICN'04, Guadeloupe", march 2004.

[40] A. TRAD, Q. NI, H. AFIFI. *Adaptive VoIP Transmission over Heterogeneous Wired/Wireless Networks*, in "MIPS04, Grenoble", november 2004.

Internal Reports

[41] V. ARYA, T. TURLETTI. *MINC and Misbehavior*, Research Report, n° 5203, INRIA, May 2004, http://www.inria.fr/rrrt/rr-5203.html.

[42] V. ARYA, T. TURLETTI, S. KALYANARAMAN. *Encodings of Multicast Trees*, Research Report, n° 5442, INRIA, December 2004, http://www.inria.fr/rrrt/rr-5442.html.

[43] C. BARAKAT, G. IANNACCONE, C. DIOT. *Ranking flows from sampled traffic*, Research Report, n° 5266, INRIA, July 2004, http://www.inria.fr/rrrt/rr-5266.html.

[44] T. BRAUN, V. ARYA, T. TURLETTI. *Explicit Routing in Multicast Overlay Networks*, Research Report, n° 5397, INRIA, November 2004, http://www.inria.fr/rrrt/rr-5397.html.

[45] H. KIM, H. AFIFI, M. HAYASHI. *EAP Bluetooth Application*, Work in Progress: <draft-kim-eap-bluetooth-00.txt>, february 2004.

[46] M. LACAGE, M. MANSHAEI, T. TURLETTI. *A Practical Approach to Rate Adaptation*, Research Report, n° 5208, INRIA, May 2004, http://www.inria.fr/rrrt/rr-5208.html.

[47] H. MEHTA, R. WALSH, V. ROCA, J. PELTOTALO, S. PELTOTALO. *FLUTE Interoperabtility Testing Guidelines*, Work in Progress: <draft-mehta-rmt-flute-iop-02.txt>, June 2004.

[48] C. NEUMANN, V. ROCA, J. LABOURÉ, Z. KHALLOUF. *An Open-Source LDPC/LDGM Large Block FEC Codec*, 2004, http://www.inrialpes.fr/planete/people/roca/mcl/.

[49] C. NEUMANN, V. ROCA, R. WALSH. *A file aggregation scheme for FLUTE*, Work in Progress: <draft-neumann-rmt-flute-file-aggregation-00.txt>, December 2004.

[50] T. PAILA, M. LUBY, R. LEHTONEN, V. ROCA, R. WALSH. *FLUTE - File Delivery over Unidirectional Transport*, IETF RMT Working Group, Request For Comments, RFC 3926, October 2004.

[51] T. PARMENTELAT, L. BARZA, T. TURLETTI, W. DABBOUS. *A Scalable ssm-based Multicast Communication Layer for Multimedia Networked Virtual Environments*, Research Report, n° 5389, INRIA, November 2004, http://www.inria.fr/rrrt/rr-5389.html.

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

[53] S. PELTOTALO, J. PELTOTALO, V. ROCA. *Simple XOR, Reed-Solomon, and Parity Check Matrix-based FEC Schemes*, Work in Progress: <draft-peltotalo-rmt-bb-fec-supp-xor-pcm-rs-00.txt>, June 2004.

[54] V. ROCA, AL.. *MCLv3: an Open Source GNU/GPL Implementation of the ALC and NORM Reliable Multicast Protocols*, 2004, http://www.inrialpes.fr/planete/people/roca/mcl/.

[55] 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° 5225, INRIA, June 2004.