Cover

instituto de telecomunicações

creating and sharing knowledge for telecommunications

Contents

Instituto de Telecomunicações - Porto 2007-2009

Welcome to IT Porto! We are a research center at the University of Porto, which is affiliated with the Instituto de Telecomunicações, a national institute with six different locations and about 150 researchers with a PhD working on a wide range of topics related to communications engineering. IT Porto was launched in January 2007 by three professors of the Department of Computer Science (João Barros, Miguel Coimbra, Miguel Rodrigues) and has since grown steadily to a full bodied institute with more than 50 members and a strong presence both in the School of Sciences (FCUP) and the School of Engineering (FEUP). By focusing on key competitive areas that span fundamental research in information theory, design of communication protocols, algorithms for multimedia processing and, more recently, security and human-computer interaction, IT Porto is well poised to become an international center of excellence in information and communication technologies, as well as in training high-potential young researchers from various parts of the world.

This brochure provides you with a sample of our most recent achievements. A lot of this research work has been carried out in close collaboration with some of the top groups in our area, based at institutions such as MIT, Princeton, Harvard, Georgia Tech, Cambridge and TU Muenchen, to name just a few. Our post-docs and PhD students routinely spend time at these institutions, thus bringing to our lab not only knowledge but also an array of best practices, which we aim to incorporate in our labs and in our institutions.

None of this would be possible without our funding agents. We are particularly grateful to the Fundação para a Ciência e Tecnologia (FCT) and the European Commission. We are also deeply involved with the Carnegie Mellon Portugal and the MIT Portugal partnerships, which are again funded by FCT. Other important sources include the Luso American Foundation, MIT and our industrial partners at NTT DoCoMo Eurolabs.

A lot of effort has gone into putting together this research portfolio. Special credits are due to Fausto Vieira and João Almeida, who gathered and edited the contributions of PhD students and senior researchers with patient perseverance. I am grateful to everyone for their excellent work.

We hope you enjoy these pages and ask that you contact us with your comments, ideas and suggestions. If this document leads to a number of exciting discussions at the white board, then our goal will have been achieved!

João Barros
Coordinator of IT Porto
jbarros@fe.up.pt

instituto de telecomunicações

Instituto de Telecomunicações,
Faculdade de Engenharia da Universidade do Porto,
Rua Roberto Frias,
4200-455 Porto, Portugal

EDITOR IN CHIEF
João Barros (jbarros@fe.up.pt)

TECHNICAL EDITORS
Fausto Vieira
(fausto.vieira@fe.up.pt)

EDITORS
Fausto Vieira
(fausto.vieira@fe.up.pt)
Tiago Vinhoza
(tiago.vinhoza@ieee.org)
João Almeida
(jalmeida@dcc.fc.up.pt)

LaTeX **TECHS**
Fausto Vieira
(fausto.vieira@fe.up.pt)

This project wishes to thank
Ana Martins and Paulo Jesus of the Divisão de Comunicação e Imagem at Faculdade de Engenharia da Universidade do Porto, as well as Gianluca Pignalberi for the excellent LaTeX starters kit.

instituto de telecomunicações

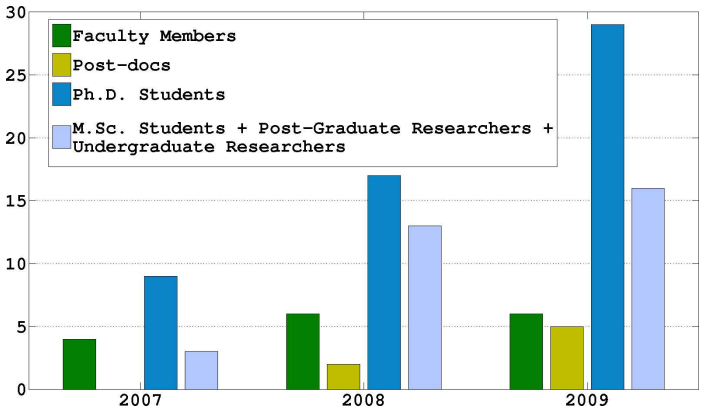
IT-Porto by the Numbers

The Porto site of the **Instituto de Telecomunicações** (IT-Porto) began its activities in January 2007 at the Department of Computer Science, Faculdade de Ciências da Universidade do Porto. Initially, the research group was composed by 4 faculty members with a Ph.D. degree and 7 Ph.D. students (including 2 assistant lecturers).

The group matured within an outstanding scientific environment, shared among researchers and students, forming a very active community which continuously captivated new research fellows and graduate students. The obvious result was the quick expansion of the Porto branch. Collaborations with foreign institutions flourished and research productivity became evident as the number of publications continued to increase at a fast pace.

Meanwhile, IT-Porto inaugurated a new laboratory, the Shannon Communications Lab, at the Department of Electrical and Computer Engineering, Faculdade de Engenharia da Universidade do Porto. The two labs, based at core schools of Universidade do Porto, allow the group to grow in a sustainable way, absorbing some of the best students graduating at these schools.

Currently, the IT-Porto site employs a total of 56 researchers, including 6 faculty members with a Ph.D. degree, 5 Post-Docs, 29 Ph.D. students (including 2 assistant lecturers), 8 M.Sc. students and 8 undergraduate and postgraduate researchers. Three administrative assistants complete the staff of IT-Porto.



Number of members of IT-Porto per year of activity.

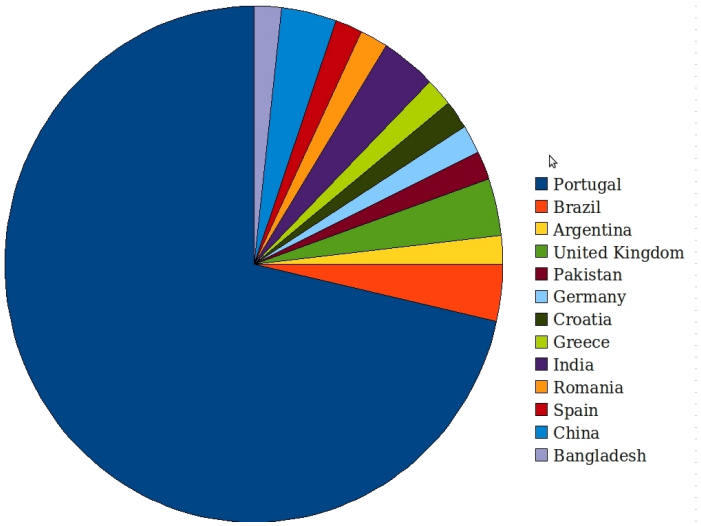
Alongside with the other IT sites, the mission of IT-Porto is the creation and dissemination of scientific knowledge in the field of telecommunications. As such, our site is actively dedicated to foster higher education by recruiting, hosting and tutoring graduate and postgraduate students, as well as creating strong bonds with foreign institutions from which they benefit on a regular basis. IT-Porto students are encouraged to collaborate with both industrial and academic partners that have a strong position in fundamental and applied research in telecommunications, both at national and international level. On the other hand, cooperation among students is cherished.

The research team

One of the main aspects that contribute to the prolificacy of research inside IT-Porto is the interdisciplinarity of its members. The inhabitance of diverse scientific backgrounds (such as Electrical and Computing Engineering, Computer Science, Network Engineering and Information Systems and Mathematics) within the group, allows researchers to work at the intersection of several research areas. This results in the emergence of innovative perspectives, not only when solving research problems but also when posing new ones.

Another of the trademarks that endows to the cultural and scientific diversity in our research group is its international orientation. Almost 30% of our research staff comes from foreign countries like Argentina, Bangladesh, Brazil, China, Croatia, England, Germany, Greece, India, Pakistan, Romania, Spain and United Kingdom.

Almost all researchers have spent some time abroad working on their Ph.D., Post-Doc. or as visiting researchers. The visited sites include the Technische Universitaet Muenchen (TUM), Cornell University, Massachusetts Institute of Technology (MIT), University College London, Cambridge University, Princeton University, Universitat Politècnica de Catalunya, Alpen-Adria-Universität Klagenfurt, Ecole Polytechnique Fédérale de Lausanne (EPFL), Carnegie Mellon University (CMU), DoCoMo Euro-Labs and Telefónica.



The nationalities of IT Porto researchers.

Research

It is all about information! The applied areas of research of our site can be summed up in 4 major topics - Information Theory, Information Networks, Information Processing and Information Security.

Under these major topics we favor more specific research domains. Research on Information Theory focuses the aspects of multi-user information theory, interplay of information/estimation theory, rate-distortion theory and network coding. Our work in Information Networks cares mostly about integration in heterogeneous networks, sensor networks, vehicular ad-hoc networks (VANETs), mobility and quality of service and small-world networks. The topics of scalable distributed compression, distributed inference, biomedical image and video processing and human computer interaction are emphasized in the domain of information processing. Physical-layer security, cooperatively secure routing, secure network coding and secret key agreement constitute the bridge between information security and our three other major areas of interest.

The broad nature of some of the research topics lead to the arrangement of several seminars and discussion groups. A weekly seminar, comprising a presentation from a student, is used for synchronization/update of the research topics that each member is working on. Additionally, there is an internal discussion group for researchers that are working on topics related to vehicular ad-hoc networks (VANETs) and a computer vision discussion group that is jointly coordinated with INESC-Porto researchers.

Research synergies are focused towards publication in journals of high impact factor and highly regarded international conferences. The IT-Porto site has managed to collect a high number of accepted publications, for such a small time existence. In the first year of existence (2007), IT-Porto researchers published 1 book chapter, 9 journal articles and 29 conference papers. In its second year 2 book chapters were published, as well as 8 journal articles and 22 conference papers. By the end of 2009, 2 book chapters, 8 journal articles and 41 conference papers had already been published or accepted for publication.

World locations where IT-Porto members presented their work.

The current project portfolio of our research group is also an extended one. We are involved in 28 ongoing projects, 17 of which a researcher from our group has the role of PI or Co-PI. Of the 28 projects, two are integrated in the partnership CarnegieMellon-Portugal and one in the MIT-Portugal international collaboration program. The internationalization of the research group can also be seen by the involvement on three European projects. The aforementioned projects are funded by entities such as FCT (Fundação para a Ciência e a Tecnologia), the European Union, Fundação Luso-Americana, the German Academic Exchange Service (DAAD), the US National Science Foundation (US-NSF) and NTT DoCoMo Euro-Labs.

Educational Activities

The faculty members belonging to IT-Porto are responsible for the following courses held at Universidade do Porto:

- Security in Systems and Networks (9th semester)
- Information Theory (8th semester / M.Sc.)
- Advanced Topics in Networks (8th semester)
- Wireless Networks (8th semester)
- Computer Vision (MSc)
- Human Computer Interaction (3rd/5th semester)
- Signal and Image Processing (MSc)
- Communication Networks (5th semester)

- Web Technologies (5th semester)
- Network Architecture Lab (6th semester)
- Computer Graphics (8th semester)
- Multimedia Systems (8th semester)

The following doctoral courses are also lectured by IT-Porto members:

- Advanced Topics in Information Security
- Information Theory
- Special Topics in Digital Communications
- Computer Vision

International Collaborations

Faculty members are also committed in bringing reputed researchers as visiting researchers to Universidade do Porto. These efforts often result in short visits by researchers from top universities around the world. Examples are of:

- Aditya Ramamoorthy (Iowa State)
- Andrea Ridolfi (EPFL)
- Andrew Thangaraj (IIT Madras)
- Angel Lozano (Universitat Pompeu Fabra)
- Daniela Tuninetti (Illinois)
- J. Nicholas Laneman (Notre Dame)
- John Baras (Maryland)
- Sir John O'Reilly (UK)
- Matthieu Bloch (Georgia Tech)
- Max Costa (Unicamp)
- Michael Gastpar (UC Berkeley)
- Muriel Médard (MIT)
- Prakash Narayan (Maryland)
- Radha Poovendran (University of Washington)
- Raymond Yeung (Chinese University of Hong Kong)
- Robert Calderbank (Princeton)
- Sergio D. Servetto (Cornell)
- Valery Khorzik (Saint Petersburg)
- Virgil Gligor (CMU)

Given the impact of research made at IT-Porto, the number of international collaborations grew quickly. Several notable researchers have become regular collaborators with IT-Porto researchers. These include:

- Andreas Demosthenous (University College London)
- Christian Bettstetter (Klagenfurt)
- Fernando Pérez-Cruz (Princeton University)
- Hideki Imai (Tokyo)
- Ian Wassell (Cambridge)
- Ioannis Chatzigeorgiou (Cambridge University)
- Izzat Darwazeh (University College London)
- J. Nicholas Laneman (Notre Dame)
- Joerg Widmer (NTT DoCoMo Euro-Labs)
- Matthieu Bloch (Georgia Tech)
- Michael Tuechler (Zurich)
- Muriel Médard (MIT)
- Ralf Koetter (TUM)
- Sergio D. Servetto (Cornell)
- Sergio Verdú (Princeton)
- Steven W. McLaughlin (Georgia Tech)

These collaborations allow the exchange of both academic and research staff.

IT-Porto Ongoing Projects

Here is a comprehensive list of the projects in which IT-Porto members participate in the role of Principal or co-Principal Investigator.

Projects in International Partnerships			
DRIVE-IN: Distributed Routing and Infotainment through VEhicular Inter-Networking	FCT (CMU-PT)	€ 900k	2009-2012
Vital Responder: Monitoring Stress in First Responder Professionals	FCT (CMU-PT)	€ 520k	2009-2011
MISC: Massive Information Scaveging with Intelligent Transportation System	FCT (MIT-PT)	€ 200k	2009-2012
Projects funded by National Institutions			
JEDI: Joint Environment for Deduction and Induction and its application over spatial data	FCT	€ 200k	2008-2010
WITS: Wireless Information-Theoretic Security	FCT	€ 130k	2008-2010
DigiScope: DIGItally enhanced stethosCOPE for clinical usage	FCT	€ 120k	2010-2012
DEWICOS Projecto da Próxima Geração de Sistemas de Comunicações Sem Fios de Débito Muito Elevado	FCT	€ 100k	2010-2012
GTI-CANE Generic Transport In Context-Aware NEtworks	FCT	€ 86k	2010-2012
Geocoding of Postal Addresses through Natural Language Techniques	QREN	€ 80k	2008-2010
FUTURE-COM: Analysis, Design and Optimization of Future Communications Systems - From Theory to Practice	IT	€ 30k	2008-2010
SECURE-COM: Physical-Layer Security From Theory to Practice	IT	€ 30k	2008-2010
Projects funded by International Institutions			
NetPEEC: Network Coding Protocols for Peer-to-Peer and Content Distribution	NTT DoCoMo Euro-Labs FCT	€ 35k	2008-2009
Foundations of Future Communications Systems: Analysis, Design and Optimization	FLAD	€ 30k	2008-2011
WiPhySec: Wireless Physical-Layer Security	US-NSF FLAD	€ 15k	2007-2009
Foundations of Future Wireless Communications Systems	US-NSF FLAD	€ 15k	2008-2010
SeNeCom: Secure Network Communications	Indian Ministry of Sci.&Tech. FCT	€ 15k	2007-2009
SENECA: Secure Network Coding and Applications	DAAD	€ 6k	2008-2010
European Projects			
N-CRAVE: Network Coding for Robust Architectures and Volatile Environments	STREP Project - FP7	€ 2.35M	2008-2010
DYNAMO: Dynamic Communication Networks: Foundations and Algorithms	COST Action	€ 450k	2005-2009
Euro-NF: Network of the Future	Network of Excellence	€ 200k	2008-2010

IT-Porto Labs

Fausto Vieira and João Barros

The IT-Porto site is branched into two laboratories. They make a bridge connection between two schools of Universidade do Porto (Faculdade de Ciências and Faculdade de Engenharia). As such, it contributes to the enhancement of the liaisons between faculty members and researchers from both institutions.

Lab at the Computer Science Department

The original IT-Porto lab is shared by Ph.D. and M.Sc. students working on Information Theory and Information Processing. Workplaces are divided among two rooms, and each workplace is equiped with its own desktop computer and file cabinet. The desktop computers are general computers that allow tasks such as the implementation of signal processing algorithms, simulations for the performance evaluation of digital communication systems and simulation of network protocols. A digital stethoscope is also available for gathering data for researchers working on biomedical signal processing. Approximately 30 TelosB sensors are also available as a sensor network testbed, mostly used for testing the network protocols, security protocols and distributed compression techniques in sensor networks.

IT-Porto lab at Faculdade de Ciências.

Shannon Communications Lab

Shannon Communications Lab was inaugurated in December 22nd, 2008. This was a cornerstone event that symbolized a new era for the IT-Porto and its expansion process. The creation of this lab was a natural outcome of João Barros' new position as an Associate Professor at FEUP. The lab is used by M.Sc and Ph.D. students, alongside post-doctoral researchers. It encompasses 14 workplaces, each one equipped with a desktop computer and personal storage space. The space encloses a gathering area, with a sofa, a coffee machine and a large LCD screen. This area is often used for welcoming visiting researchers, as well as a point for the spare moments of researchers.

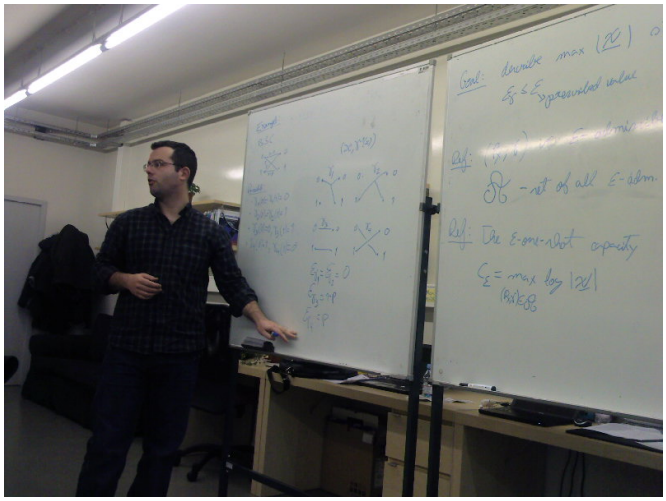
The lab is equiped with a server farmed used to process computationally demanding simulations. In addition, several notebooks with wireless interfaces are used as an ad-hoc network testbed. Five LinkBird MX radios are available for field experiments in vehicular networks. These radios have been used to gather measurements regarding signal quality, as well as to implement several applications that have high bandwidth requirements, such as real time videostreaming between moving vehicles.

Shannon Communications Lab.

Christmas dinner.

Coffee break.

DCC lab back in 2007.



Seminar by Rui Costa in Shannon Communications Lab.

Outdoor activities.

IT-Porto Team

The IT-Porto team has grown very quickly in the last two years and new members are already in the process of joining the team. Moreover, there is an active recruiting effort for several research positions that already have guaranteed funding. IT-Porto has a very high acceptance rate of project proposals in open calls, which reflects in the large number of new projects starting in 2009. All these projects ensure funding for different research positions ranging from undergraduate student up to post-doctoral researchers. A short bio of the current members is shown here.

Faculty

João Barros is an Associate Professor at the Department of Electrical and Computer Engineering of the School of Engineering of the University of Porto and the coordinator of the Porto Laboratory of the Instituto de Telecomunicações. He is also a Research Affiliate with the Massachusetts Institute of Technology (MIT). In February 2009, Dr. Barros was appointed National Director of the CMU-Portugal Program, a five-year international partnership between Carnegie Mellon University and 12 Portuguese Universities and Research Institutions, with a total budget of 56M Euros. He received his undergraduate education in Electrical and Computer Engineering from the University of Porto (UP), Portugal and Universitaet Karlsruhe, Germany, until 1999, and the Ph.D. degree in Electrical Engineering and Information Technology from the Technische Universitaet Muenchen (TUM), Germany, in 2004. From 2005 to 2008, João Barros was an assistant professor at the Department of Computer Science of the School of Sciences of the University of Porto. The focus of his research lies in the general areas of information theory, communication networks and data security. Dr. Barros received a Best Teaching Award from the Bavarian State Ministry of Sciences, Research and the Arts, as well as scholarships from several institutions, including the Fulbright Commission and the Luso-American Foundation. He held visiting positions at Cornell University and the Massachusetts Institute of Technology, where he spent a sabbatical in 2008. Beyond his duties as Secretary of the Board of Governors of the IEEE Information Theory Society, his service included co-chairing the 2008 IEEE Information Theory Workshop in Porto, Portugal, and participating in several Technical Program Committees, including ITW 2009, WiOpt (2008 and 2009), ISIT 2007, IS 2007, and IEEE Globecom (2007 and 2008).

Miguel Rodrigues received the Licenciatura degree in Electrical Engineering from the Faculty of Engineering of the University of Porto, Portugal in 1998 and the Ph.D. degree in Electronic and Electrical Engineering from University College London, U.K. in 2002.

From January 2003 to September 2006, he held postdoctoral research appointments at Cambridge University, U.K., both as a Research Associate and later as a Senior Research Associate. From September 2006 to March 2007, he was a Visiting Researcher at Princeton University, U.S.A. In March 2007, he joined the Department of Computer Science, Faculty of Sciences of the University of Porto, as an Assistant Professor, and he also joined the Instituto de Telecomunicações. He is an Honorary Senior Researcher at University College London, U.K. he has also been a Visiting Researcher at Princeton University, U.S.A. in the Summer of 2007 and 2008.

His research interests include the general areas of information theory, communications theory, signal processing and optimization, and their applications to wireless and optical systems and networks. He has over 70 publications in international journals and conference proceedings in these areas. He has also been lecturing frequently abroad and has also served as a technical consultant to major international telecommunication companies.

He has served on the technical programme committee of various international conferences. He was the recipient of the the Prize Engenheiro António de Almeida, the Prize Engenheiro Cristiano Spratley, and the Merit Scholarship from the University of Porto, and the best student poster prize at the 2nd IMA Conference on Mathematics in Communications. He was also the recipient of doctoral and postdoctoral fellowships from the Portuguese Foundation for Science and Technology, and postdoctoral fellowships from Foundation Calouste Gulbenkian.

Miguel Tavares Coimbra was born in Porto, Portugal in 1975. He received his B.Sc. in Electrical Engineering and Computers in Faculdade de Engenharia da Universidade do Porto in 1998. He worked in 1999 at INESC-PORTO as a researcher. In 2000 he began his Ph.D. studies in King's College London in the area of computer vision. He transferred to Queen Mary, University of London in 2002, where he concluded his Ph.D. studies in 2004. He worked as a post-doc researcher in medical imaging at IEETA-Universidade de Aveiro in Portugal until September 2006. He is currently a lecturer at Faculdade Ciências da Universidade do Porto in Portugal.

Rui Prior received the Licenciatura and M.Sc. degrees in Electrical and Computer Engineering from the Faculty of Engineering of the University of Porto in 1997 and 2001, respectively, and the Ph.D. in Computer Science from the Faculty of Sciences of the University of Porto in 2007. In 2000 he was awarded a Praxis XXI Programme M.Sc. fellowship by the Portuguese Foundation for Science and Technology (FCT). He is currently an Assistant Professor at the Department of Computer Science of the Faculty of Sciences of the University of Porto and a researcher at the Networking and Information Processing Group of the Instituto de Telecomunicações. He had previously worked as a researcher in the Telecommunications and Multimedia Unit of INESC-Porto and in the Information Networks Group of the Laboratory of Artificial Intelligence and Computer Science (LIACC). His research interests are in the field of data communication networks and protocol engineering. Rui Prior has worked in several projects funded by the European Union — N-Crave (FP-7), Daidalos (FP-6), Atlantic (FP-4) — and in other projects of national scope. He is a member of the ACM, IEEE and IEICE.

Verónica Costa Orvalho born in 1976, mother of a lovely boy. Holds a Ph.D. in Software Development (Computer Graphics) from Universitat Politècnica de Catalunya (2007), where her research centered on "Facial Animation for CG Films and Videogames". She has been working in IT companies, such as IBM and Ericsson, and Film companies, like Patagonik Film Argentina since 1994. She has given many workshops and has international publications related to game design and facial animation in conferences like SIGGRAPH and Symposium in Computer Animation. She has received international awards for several projects: "Photorealistic facial animation and recognition", "Face Puppet" and "Face In Motion". Now, she is a full time professor at University of Porto and cofounder and CTO of Face In Motion (http://www.faceinmotion.com). She is also a former research member at the Event Computational Lab (http://moving-event.org/) working on virtual reality and character animation. Current and past collaborations include several film and game companies (Blur Studios, Electronic Arts, Microsoft Portugal, Dygra Films), and research groups (Stanford University, Universitat Politècnica de Catalunya). Her current research focus on developing new methods related to motion capture, geometric modeling and deformation, and real time animation. She has participated as a reviewer and as program committee member in high impact conferences and journals like SIGGRAPH, IEEE Virtual Reality and Computer and Graphics among others.

Michel Ferreira received his B.Sc. in Applied Mathematics - Computer Science, from Faculdade de Ciências da Universidade do Porto, in June 1994. He received his M.Sc. degree in Computer Science from the Department of Computer Science, Universidade of Minho, Portugal, in October 1996. He obtained his Ph.D. degree in Computer Science at the Department of Computer Science, Faculdade de Ciências da Universidade do Porto, in April 2002. He is an Assistant Professor and since 1995, was a researcher at the Laboratory of Artificial Intelligence and Computer Science, before joining the Instituto de Telecomunicações, in 2009.

Post-Doctoral researchers

Fausto Vieira was born in Porto, Portugal. In 2001, he received his Licenciatura in Computer and Electrical Engineering from FEUP. After working for a short period for a consulting company, he went to the Netherlands to work for the European Space Agency (ESA), in the Telecommunications Section. There he was a technical officer for several ESA awarded projects, besides performing satellite systems field trials and experiments. In 2004, he enrolled in the Telematics Engineering Ph.D. program at the UPC in Barcelona. His Ph.D. thesis "Quality-of-Service Provision for Satellite Systems implementing Adaptive Physical Layer" reflects his contribution to an ESA awarded project, where he was part of the winning consortium. In Sept. 2008, he became a post-doc researcher at IT-Porto and he is part of several international projects.

Ian Marsh was born in the UK in 1965. He received a joint B.Sc. in Physics and Computer Science in 1987 from the Metropolitan University of Manchester. Subsequently, he received his M.Sc. in Systems Design from the University of Manchester in 1988. Since then, he has worked at the CSIRO in Australia and IBM in Germany. For the past 12 years he was worked at the Swedish

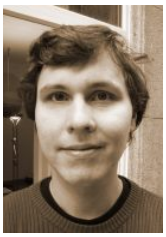
Institute of Computer Science (SICS) working on real-time networking issues and defended his Ph.D. in June 2009 on the topic of 'Quality aspects of Internet telephony'. On 1st of July 2009 he joined the NIP group as a post-doctoral researcher, where he works on large-scale dissemination and vehicular networks.

Tiago T. V. Vinhoza received his diploma, M.Sc. and Ph.D. degrees in Electrical Engineering from the Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) in 1999, 2003 and 2007, respectively. Mr. Vinhoza's doctoral dissertation was on structures and adaptive algorithms for blind CDMA interference suppression. He devised new blind adaptive algorithms for parameter estimation and proposed receiver structures for interference mitigation. Mr. Vinhoza had also several collaborations with other students from his former research group at PUC-Rio, mainly on single carrier block transmission systems, OFDM and multicarrier CDMA. Since 2008, he is a Postdoctoral Researcher in the Networking and Information Processing Group (NIP) of the Instituto de Telecomunicações (IT–Porto) where he is doing research on wireless information-theoretic security.

William Carson was born in Coventry in the West Midlands. He was educated at King Henry VIII School and read Engineering at Queens' College, Cambridge, where he was awarded a MEng degree in 2005. He has just completed his Ph.D. entitled "Performance modelling and design of bit-interleaved coded modulation systems over quasi-static fading channels" at the Computer Laboratory, University of Cambridge under the supervision of Dr. Ian Wassell from the Computer Laboratory and he was further advised by Dr. Miguel Rodrigues at the University of Porto. He is currently a post-doctoral researcher at the University of Porto under the supervision of Dr. Rodrigues, as well as Dr. Fernando Perez-Cruz from Princeton University.

Ph.D. students

Diogo Ferreira is a Ph.D. student in MAP-tele Doctoral Programme in Telecommunications and a researcher at Instituto de Telecomunicações. His main areas of interest are information dissemination over wireless channels, large-scale network simulation, impact of topology and network coding protocols. He is also a key software developer of the NECO simulation platform.



Gerhard Maierbacher is currently a Ph.D. student at the Department of Computer Science, University of Porto (UP), Portugal, under the supervision of Prof. João Barros. He received his M.Sc. degree at the Technische Universität München (TUM), Germany, where his thesis was supervised by Prof. Joachim Hagenauer and Prof. João Barros at the Institute for Communications Engineering. In 2006 he was awarded a Ph.D. scholarship by the Portuguese Foundation for Science and Technology and started his research at the Instituto de Telecomunicações (IT), Portugal, which is focused on low-complexity source, channel and network coding strategies for wireless sensor networks. Since then, he has been involved in several international projects (SIGaPano, WITS, N-Crave) and regularly performs reviews for IEEE journals and conferences. In 2008, he was a visiting student with Prof. Muriel Médard at the Massachusetts Institute of Technology (MIT), USA. In 2009, he was working with Prof. Christina Fragouli at the École Polytechnique Fédérale de Lausanne (EPFL), Switzerland. His practical expertise includes a skilled worker degree as electronic technician with Rohde & Schwarz, Germany, and work experience at the esz-Kalibrierlabor, the Fraunhofer Institute, and Cosiro, Germany. During his M.Sc. studies he did internships at the Fraunhofer Institute, Germany, as well as at the Lappeenranta University of Technology (LUT), Finland.

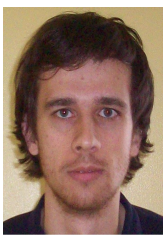
João Almeida received his B.Sc. and M.SC. degrees in Computer Science from Faculdade de Ciências da Universidade do Porto, in 2007 and 2009, respectively. He is a Ph.D. candidate in the MAP-tele program, held at Faculdade de Engenharia da Universidade do Porto. In 2008 he joined the Networking and Information Processing Group (NIP) affiliated with Instituto de Telecomunicações (IT), and has been a researcher there since then. He is working on the intersection of coding theory with cryptography, more specifically in secure code design. His research interests include information theory, security and algorithm design.

João P. Vilela is currently pursuing the Ph.D. degree at the Universidade do Porto (UP), Porto, Portugal. He is a Researcher in the Networking and Information Processing Group (NIP) of the Instituto de Telecomunicações (IT), where he has been since 2005. His research interests include mobile ad-hoc networks, physical-layer security and cooperation in wireless networks. He received the Doctoral Scholarship from the Portuguese Foundation for Science and Technology.

João Rodrigues is a researcher at Instituto de Telecomunicações - Porto, under the supervision of Prof. Dr. João Barros. He received his Masters degree in Electrical and Computer Engineering from the Faculdade de Engenharia da Universidade do Porto (UP), in July 2009. He is currently enrolled in the Doctoral Program MAP-Tele, and he has been awarded a FCT Ph.D. scholarship. His research interests are Sensor Networks, Information Dissemination and Intelligent Networks.

Luísa Lima is currently pursuing the Ph.D. degree at the Universidade do Porto (UP), Porto, Portugal. She is a Researcher in the Networking and Information Processing Group (NIP) of the Instituto de Telecomunicações (IT), where she has been since 2005. She also collaborates regularly with the Research Laboratory of Electronics at MIT. She was awarded the Doctoral Scholarship from the Portuguese Foundation for Science and Technology. Her research interests include network coding, security, random graphs, video streaming and computer simulation.

Maricica Nistor was born in Iasi, Romania. She received her Engineer's Degree at Technical University of Gh. Asachi, Electronics and Telecommunications Faculty, Romania in 2007, and her Master's degree at the same university in 2008. She started her Ph.D. in November 2008 at University of Porto, Portugal, under the supervision of Prof. João Barros. Her research interests lie on the general areas of Network Coding and Digital Communications.



Mate Boban received his Diploma in Informatics (highest honors) from University of Zagreb, Croatia, in 2004. In Feb. 2005, he enrolled in the postgraduate program in Telecommunication and Informatics, University of Zagreb, at the same time working as a teaching/research staff at the Faculty of Organization and Informatics, University of Zagreb. In 2007, he received a Fulbright pre-doctoral scholarship, which he utilized in the Dept. of Electrical and Computer Engineering, Carnegie Mellon University from

August 2007 until January 2009. Since March 2009, he is a Ph.D. student in the dual Carnegie Mellon-Portugal Program. His current research interest is in the area of Vehicular Ad Hoc Networks (VANET).

Paulo F. Oliveira received his undergraduate education in Network Engineering and Information Systems from the Universidade do Porto (UP), Portugal, until 2006. He is currently pursuing the Ph.D. degree in the same University and he is a Researcher in the Networking and Information Processing Group (NIP) of the Instituto de Telecomunicações (IT), where he has been since 2007. His research interests include security, sensor networks, information theory, and communication networks. Mr. Oliveira received the Doctoral Scholarship from the Portuguese Foundation for Science and Technology and the Prize Engenheiro António de Almeida (Best Student Award).

Pedro Santos was born in 1986 at Oporto, and graduated from Universidade do Porto in Electrical and Computer Engineering in 2009. Currently he is pursuing Ph.D. studies at the Network and Information Processing Group (NIP), at Instituto de Telecomunicações (IT). He received a Doctoral Scholarship from the Portuguese Foundation for Science and Technology, and his interests at this point are Wireless Sensor Networks.

Rui A. Costa received his undergraduate education in Applied Mathematics at the Universidade do Porto - best student in the 2006 class - and the Masters degree in Informatics (Branch of Systems and Networks) at the same University in 2007. He is currently a Ph.D. student at the same University and he received the Doctoral Scholarship from the Portuguese Foundation for Science and Technology. Since 2006, he is a Researcher in the Networking and Information Processing Group (NIP) of the Instituto de Telecomunicações (IT). From September to December 2007, he was a Working Student at DoCoMo Euro-Labs in Munich. The focus of his research lies in complex network analysis and in network coding for wireless networks, with special focus to delay sensitive applications.

Rui Meireles received his Informatics and Computing Engineering degree from the University of Porto, Portugal in 2006. Starting from 2007 he is a Computer Science Ph.D. student of the Portuguese MAP consortium and Carnegie Mellon University, part of the CMU-Portugal partnership program, funded by the Portuguese Foundation for Science and Technology. His current research is in the area of Vehicular Ad-Hoc Networks (VANETs), but his interests extend to Computer Systems and Software Engineering as well.

Saurabh Shintre hails from India and received his Bachelor & Master of Technology in EE from the Indian Institute of Technology Bombay, Mumbai. He is currently a Ph.D. candidate in the MAP-tele program at Faculdade da Engenharia, U.Porto and has been with the group since September, 2009. His research interests are information theory, network coding, compressed sensing for networks. His has also worked as summer researcher at the Chinese University of Hong Kong and has published works on Real and Complex Network Codes.

Sérgio Crisóstomo is currently an Assistant Lecturer from the Computer Science Department of the School of Sciences from the University of Porto. He studied Electrical and Computer Engineering at the School of Engineering from the University of Porto, where he graduated and received the M.Sc. degree in 1997 and 2003, respectively. Since 2006 he is doing its Ph.D. research both at the University of Porto, under the supervision of Prof. João Barros, and at the Alpen-Adria-Universität Klagenfurt, Austria, under the supervision of Prof. Christian Bettstetter. His Ph.D. work focus Information Dissemination in Random Networks including Network Coding based approaches, for which he has been granted a scholarship from the Fundação para a Ciência e Tecnologia (FCT), Portugal. From 1997 to 2002 he worked as a researcher at INESC-Porto, and from 2002 to 2006 he was a researcher at the Laboratório de Inteligência Artificial e de Ciência de Computadores (LIACC). In January 2007 he joined the Porto Laboratory of the Instituto de Telecomunicações. He is a student member from ACM and IEEE since 2006.

Pedro Brandão is currently an assistant lecturer at the Computer Science Dept. of the School of Sciences in the University of Porto. He is pursuing a Ph.D. degree at the Computer Laboratory, University of Cambridge under the topic of Body Sensor Networks, for which he has been granted a scholarship from the Fundação para a Ciência e Tecnologia of Portugal. He did his diploma and M.Sc. (ECE) at the Engineering School of the University of Porto and has worked in Research at IT-Aveiro, PT Inovação, INESC-Porto, LIACC and since 2007 in IT-Porto. He is a student member of ACM and IEEE since 2006. Current research interests include sensor/actuator networks and protocols specific for the human body and middleware architectures.

Ioannis Kanaras was born in Athens, Greece. He received his BSc from the National Technical University of Athens, Athens, Greece in 2001 and his M.Sc. degree from the University College London, London, UK in 2002, all in electrical engineering. From 2004 to 2007 he worked for Siemens Greece. He is currently working in the University College of London towards his Ph.D. degree under the supervision of professors Izzat Darwazeh and Miguel Rodrigues of University College London, London, UK and University of Porto, Portugal, respectively. His research interests include transmission techniques, optimization algorithms and detection methods applied in multicarrier communication systems.

João Oliveira received his "Licenciatura" degree in Electrical Engineering from the Faculdade de Engenharia da Universidade do Porto, Portugal, in 2005. he is presently working towards his Ph.D. degree in Electrical Engineering, in the Faculdade de Engenharia da Universidade do Porto in collaboration with the Instituto de Engenharia de Sistemas e Computadores do Porto. My main current research interests include optical communications, wireless-over-fiber networks and multicarrier modulation techniques.

Ke Zhang is from China. She received her B.Sc. degree in Communication Engineering in Shanghai University, China in 2007 and a M.Sc. degree in Communication and Information Systems in Huazhong University of Science and Technology, China, in 2009. Currently she is working towards a Ph.D. degree from Department of Computer Science in Porto University. She is an IT-Porto researcher.

Munnujahan Ara received her B.Sc. degree and her M.Sc. degree in Mathematics from the university of Khulna in Bangladesh in 2003 and 2005, respectively. Currently she is working towards a Ph.D. degree from the MAP-tele doctoral program. She is also an IT-Porto researcher.

Vinay Prabhu received the B.Engg. Degree in Electronics and Communications from BMS College of Engineering, Bangalore in 2005 and M.Sc. (By Research) degree in Electrical Engineering (Specialization: Wireless Communications) from Indian Institute of Technology, Madras in 2008. Currently he is working towards a Ph.D. degree in the MAP-I program and is also an IT-Porto researcher.

Ye Can received the B.Sc. degree in Information Engineering from Zhejiang University, China, in Jun. 2008. He has been enrolled in CMU-Portugal Dual Ph.D. program and was awarded a CMU-Portugal Fellowship. For the time being, he is working towards the Ph.D. degree in Electrical & Computer Engineering at Carnegie Mellon University and the Ph.D. degree in Computer Science at University of Porto.

Fábio de Lima Hedayioglu was born in Juazeiro, Brazil in 1980. He received his B.Sc. in Computer Science in Universidade Federal de Pernambuco in 2005. As a B.Sc. student, developed a telemedicine system at the Royal Portuguese Hospital in Recife, Brazil, and took part in several national-wide research projects regarding medical informatics. He worked in 2006 at C.E.S.A.R. in several projects with Samsung and Dell, as software engineer. He began his M.Sc. in Medical Informatics at Faculdade de Medicina da Universidade do Porto in 2007. Currently he is finishing his M.Sc. and is a MAP-i Ph.D. student. His main interests are biomedical image processing, biomedical signal processing and bioinformatics.

Farhan Riaz finished his graduation from National University of Sciences and Technology, Pakistan. He went to Technical University of Munich, Germany for doing his Master's. Currently he is a Ph.D. student, working under the supervision of Prof. Miguel Tavares Coimbra.

Ana Teresa d' Oliveira Campaniço is a Ph.D. student in Computer Science at the University of Trás-os-Montes e Alto Douro (UTAD) / University of Porto (UP). She has a M.Sc. in Computer Games Development (Letterkenny Institute of Technology - LYIT, Ireland) and another in Computer Science (UTAD, Portugal), both in 2008 (one in January and the other in December, respectively). Although she is a programmer with interests in computer graphics, evolutionary algorithms and other nature inspired methods, she actually came from a strong artistic background. She has professional experience as a freelance artist and has participated in the production of some games. She is proficient in English.

Bruno Oliveira is a Ph.D. student of the MAP-i doctoral programme in computer sciences. He has a B.Sc. in Computer Science, and is waiting for the oral presentation of his M.Sc. in computer graphics, which focus on real-time graphics. Parallel to the Ph.D., he works at the University of Minho as a grant researcher in the area of grid computing. Almost his entire career was dedicated to research, either in research facilities, such as CCG (Computer Graphics Centre) of University of Minho, or in his co-owned company, doubleMV – Research and Development.

José Carlos Miranda obtained his M.Sc. in Tecnologia Multimédia from the Faculdade de Engenharia da Universidade do Porto (FEUP), in 1999. He is currently enrolled in the Ph.D. program in Informatics Engineering at FEUP and his research is focused on *Interaction between virtual characters and humans or others avatars in rehabilitation domain*. He is also an assistant lecturer at the Departamento de Informática da Escola Superior de Tecnologia e Gestão do Instituto Politécnico da Guarda, since 1995.

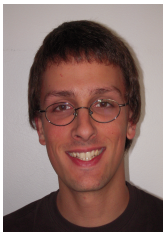
Hugo Conceição was born and raised in Albergaria-a-Velha, a small town near Aveiro, Portugal, in 1985. In 2004, he moved to Oporto, Portugal, to study Computer Science at University of Porto , Faculty of Science. Since 2006, he is a researcher at LIACC and Instituto de Telecomunicações under the supervision of Professor Michel Ferreira and Professor João Barros. He received my diploma in 2008. In 2009 he was accepted in the dual Carnegie Mellon - Portugal Ph.D. program.

Pedro Gomes was born in 1985 in Matosinhos, Portugal. In 2009, he received his M.Sc. degree in Network and Information Systems Engineering from Faculty of Sciences of the University of Porto. He is a Ph.D. student of the MAP-i Doctoral Programme in Computer Science and a researcher at the Instituto de Telecomunicações. His main areas of interest are Telecommunications, Spatial Databases, Navigation Systems, and Distributed Systems. His main research topic is Vehicular Ad-Hoc Networks (VANETs).

Ricardo Fernandes was born in 1984 in Bragança, Portugal. He received his M.Sc. degree in Network and Information Systems Engineering from the Department of Computer Science of the University of Porto (DCC-FCUP). Currently, He is a Ph.D. student of the MAP-Tele Doctoral Programme in Telecommunications and a researcher at the Instituto de Telecomunicações. His main areas of interest are Telecomunications, Distributed Systems and Spatial Databases. His main research topic is Vehicular Ad-Hoc Networks (VANETs).

M.Sc. students

José Serra is currently pursuing the M.Sc. degree in Network and Information Systems Engineering - branch of Distributed Systems - at Faculty of Sciences of University of Porto. He's been working as a developer of the NECO (NEtwork COding) simulator. Currently his main interests in general are computer graphics, networks and software development.



Gil Ramos was born in 1986 in Porto. In 2007, he obtained his degree in Mathematics from the Faculdade de Ciências da Universidade do Porto and continued on to pursue a M.Sc. in Mathematics. In 2005/06, he obtained a scholarship from the Gulbenkian Foundation within the New talents in Mathematics program. He is currently a researcher in a Fundação para a Ciência e Tecnologia (FCT) funded project at IT-Porto.

Bruno Lopes is an IT/IBMC researcher. He is enrolled at the University of Porto as a M.Sc. student on the Masters of Computer Science programme. He has a degree in Computer Science. In 2008, while working at IBMC, he developed a software to help improve Leishmania studies. Current research interests include the areas of Computer Vision and Software Architecture.

Nuno Barbosa holds a BSc in Computer Science from Faculdade de Ciências da Universidade do Porto and he is an amateur cellist. For the past few years, he has been involved with projects in Computer Graphics, Facial Animation and Videogames programming, such as implementing an engine for facial animation in Xbox360. Also, he has made research and developed tools for e-Learning. Now, he has a research scholarship at Centro de Cálculo, Faculdade de Ciências da Universidade do Porto, where he creates tools for content integration between different databases systems and different web platforms, and he is currently finishing is M.Sc. in Computer Science (July 2010).

Ricardo Castro was born in 1984 in Oporto. He is currently pursuing the M.Sc. degree at the Universidade do Porto (UP), Porto, Portugal in the field of Parallel and Distributed Systems. His research interests include databases and logic programming.

Administrative staff

Silvia Bettencourt Ribeiro works for several years with the University of Porto, in three different departments and schools. Her most recent position is Office Manager in the Instituto de Telecomunicações, Porto (IT-Porto), which involves work with Scientific R&D Projects, based on institutional procedures of the Portuguese Foundation for Science and Technology (FCT), as well as European guidelines. Her work focuses on financial and administrative tasks, which includes budget control, grant research and scholarship contracts, reporting directly to the Coordinator of IT-Porto. During her time at IT-Porto, Silvia played a key role in the organization of the IEEE Information Theory Workshop 2008. She holds a post-graduate degree in Information Systems from the School of Engineering of the University of Minho and graduated on Public Administration from the School of Economics and Management of the same university. She also holds the level of Certified Accountant, granted by the Portuguese Chamber of Official Auditors.

Before working at Instituto de Telecomunicações, Porto (IT-Porto), **Sara Armas** worked with Qimonda Portugal, SA at the Purchasing Department. She was involved in some projects such as continuous improvement of the database. She was also responsible for training new office colleagues, interfacing between the accounting and other departments, making data follow ups and managing contracts, supplies and material data. She is graduated in Assessoria de Gestão from the Instituto Superior de Contabilidade e Administração do Porto.

Elimary Silva has a Degree in Management from University of Minho. Before joining Instituto de Telecomunicações, Porto (IT-Porto), she worked for 5 years as a Scholarship Manager at the AlBan Office, the office responsible for the implementation of Programme AlBan, a high level scholarship programme specifically addressed to Latin America.

instituto de telecomunicações

Research Topics

Network Coding Multicast in Satellite Networks

Fausto Vieira and João Barros

The broadcast nature of satellite networks such as DVB-RCS based systems provides a highly effective medium for content distribution, especially in the case of geographically scattered clients. Non-real-time services typically rely on application level protocols that often use forward error correction (FEC) and carousel data cycling schemes in unidirectional links. The presence of a feedback channel in satellite networks is mostly unexploited in the context of reliable multicast services. We show that network coding protocols offer a native and transparent solution for reliable multicast over satellites. When employing a feedback channel, network coding can reach near real-time performance at an efficiency level close to known theoretical bounds for lossy satellite links.

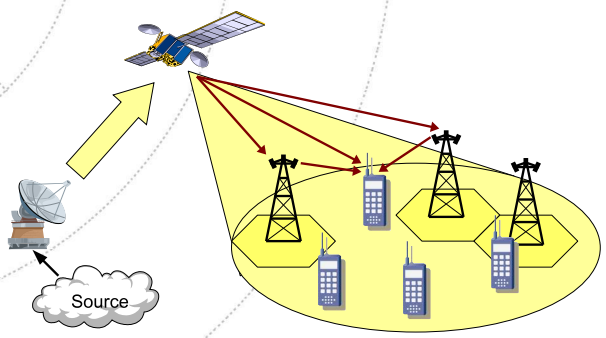
Introduction

In the context of communication networks and protocols, network coding [1, 2] offers a disruptive networking concept: data throughput and network robustness can be considerably improved by allowing the intermediate nodes in a network to mix different data flows through algebraic combinations of multiple datagrams. This key idea clearly breaks the classical networking paradigm where intermediate nodes are only allowed to store and forward packets. This concept is particularly relevant for satellite networks where erasure patterns in large terminal populations can be countered by broadcasting encoded packets to multiple nodes simultaneously until the destination nodes have enough degrees of freedom to decode and recover the original data.

Reliable multicast has been a key satellite-based service for many years due to the inherent broadcast nature of satellite communications. Content distribution is one of the key applications for reliable multicast services.

Network coding has shown to be especially useful over wireless networks, in aspects such as mobility, multipath, security and multicasting.

Terrestrial-based solutions for content distribution have recently gained traction, mostly due to the ever decreasing costs of broadband communications, associated with disruptive technologies such as peer-to-peer content distribution. Nonetheless, satellite-based platforms present many important advantages that are difficult to match.



Multipath scenario in mobile satellite networks

First of all, the scalability is guaranteed due to the broadcast nature of satellite communications. Moreover, satellite networks are designed to support very large terminal populations. Second, terrestrial infrastructure independence is provided by the satellite coverage ubiquity. In fact, satellite terminals can provide Internet access for remote locations or in moving vehicles such as trains and planes. Third, the typical star topology in satellite networks simplifies multicast services since there is no routing within the satellite segment. Finally, bandwidth management is usually trivial to most satellite systems, which is quite important when designing a content distribution platform.

Our main contributions are two-fold: (1) efficiency improvements in reliable multicast and (2) very low decoding delay. The first originates from the algebraic mixing of different packets, which increases the likelihood that received packets carry new information. Moreover, channel diversity minimizes redundancy in the recovery data. When comparing with fountain codes, a very low decoding delay is possible due to closed-loop network coding scheduling algorithms.

The impact of this approach is also two-fold: first, it provides a transparent solution for reliable multicast, which means that specific transport or application level protocols are no longer required; second, it allows for erasure-free streaming multicast, even with a long transmission path delay that is characteristic in satellite networks. The decoding delay is within the same order of magnitude as the buffering delay employed by Internet streaming applications.

Network Coding Multicast in Satellite Networks

Network coding has shown to be especially useful over wireless networks, in aspects such as mobility, multipath, security and multicasting. Since satellite systems have very specific characteristics, we will present how network coding is employed in wireless networks and explain later how it is applied to satellite specific scenarios. These scenarios shall provide the basis for a framework for network coding in satellite systems.

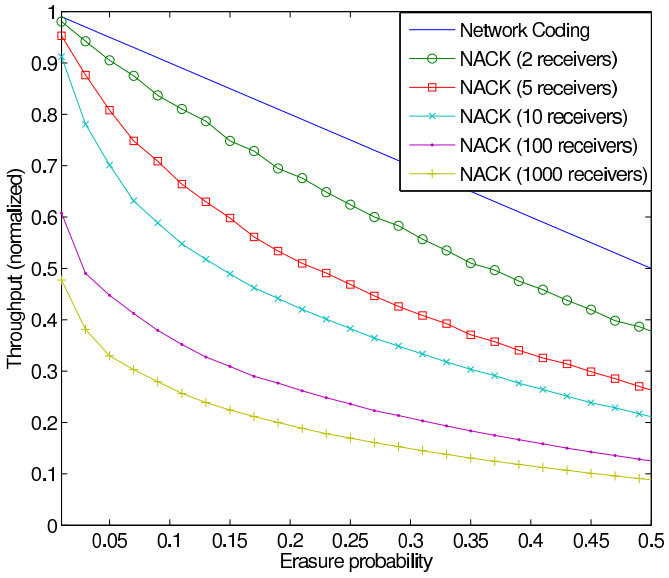
Performance Gains

The performance gains are focused in comparing the previously presented network coding multicast scenario to the traditional NACK-based reliable multicast. With network coding multicast, each node only needs to receive enough symbols in order to successfully decode the data. However, in traditional NACK-based reliable multicast, each node must successfully receive every symbol that is transmitted. Therefore, as the number of receivers increases the overall efficiency is reduced.

This clearly presents serious scalability issues, as shown in previous figure. Note that Satellite Networks can cover very wide geographical areas with large number of terminals and therefore scalability is a fundamental performance indicator for these systems [3, 4].

Conclusion

The presented network coding multicast for Satellite Networks was shown to be applicable to both fixed and mobile terminals. The proposed solution limits the role of network coding to the satellite segment, since the network coding protocol would be included in the encapsulation protocol. This brings important advantages in terms of deployment and transparency to upper layers as well as to external network segments. Furthermore, the simulation results show great improvements in terms of performance between traditional and network coding approaches. This performance is more relevant for scenarios with a large number of terminals, which is the case for most satellite systems.



Network coding multicast is independent of the number of receivers since it only requires that each node receives enough symbols in order to decode the data. On the other hand, NACK-based multicast requires that each node receives every symbol in order to decode the data.

We demonstrated that network coding can take advantage of the feedback channel in Satellite Networks in order to reach performances close to the theoretical bounds.

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *Information Theory, IEEE Transactions on*, vol. 46, no. 4, pp. 1204–1216, Jul 2000.

[2] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *41st Allerton Conf. Communication, Control and Computing*, Monticello, IL, US, Oct 2003.

[3] F. Vieira and J. Barros, "Network coding multicast framework for broadband satellite systems," in *7th Conference of Telecommunications*. Santa Maria da Feira, Portugal: Instituto de Telecomunicações - Aveiro, May 2009, p. 390.

[4] ——, "Network coding multicast in satellite networks," in *accepted to the 5th Euro-NGI Conference Next Generation Internet Networks*. Aveiro, Portugal: Instituto de Telecomunicações - Aveiro, July 2009.

NECO: NEtwork COding Simulator

Diogo Ferreira, Luísa Lima and João Barros

We present NECO, a high-performance simulation framework dedicated to the evaluation of network coding (NC) based protocols. Its main features include: (1) definition of graphs representing the topology (which can be generated randomly or predefined by means of a standard representation), (2) modular specification of network coding protocols, (3) visualization of the network operation and (4) extraction of key statistics. The simulator is entirely written in Python and can be easily extended to account for extra functionalities.

Introduction

The key insights of [1], which proved that the max-flow min-cut capacity of a general multicast network can only be achieved by allowing intermediate nodes to mix different data flows, has caused a surge in *network coding* research (e.g. [2, 3]) uncovering its potential to provide higher throughput and robustness, particularly where highly volatile networks such as mobile ad-hoc networks, sensor networks and peer-to-peer networks are concerned. Network coding simulation presents the following significant main challenges in comparison to traditional routing protocols:

- Since network coding is particularly beneficial in unreliable and large networks, the simulator must be capable of reproducing the dynamics of complex networks, that is, networks with a very large number of nodes, in an efficient way;
- Because protocol stacks for network coding are yet to be defined, the simulator should be as generic as possible, such that many features of classical network simulators become excessive and should be avoided.

Our main contribution is NECO (Network Coding Simulator), a first step towards a common core for a high-performance open-source simulator for the network coding scientific community. It is entirely written in Python and allows for the evaluation of network coding based protocols. It is easily extensible and allows for high-performance simulation in complex networks.

Features and Usage

NECO is aimed at the evaluation of network coding based protocols. The capabilities of NECO can be sub-divided in two groups: (a) pre-implemented features and (b) extensions, such as external plugins. A typical usage of the simulator, both in graphical and text modes, can consist of the generation of a graph and selecting sink(s) and source(s), followed by the determination of the routing and network coding protocol, and the visualization of the network operation in real-time. The latter uses either the graphical user interface or the text output at the terminal. Simulation data can be extracted by interpreting the statistics file that is generated in a seamless fashion.

> NECO is a first step towards a common core for a high-performance open-source simulator for the network coding scientific community.

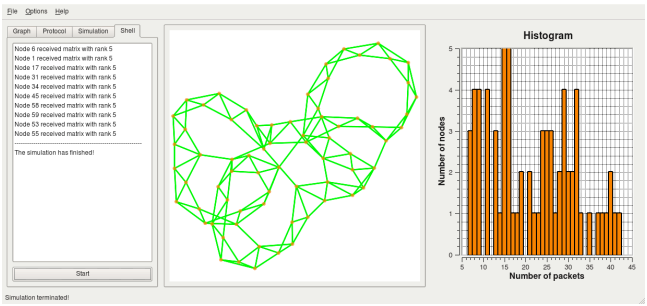
User features, interfaces and output

NECO's main pre-implemented features include:

1. Generation of random graphs and optional import of graphs in the standard *graphviz* format;
2. Basic flooding and network coding protocols, among which several versions of the Random Linear Network Coding protocol;
3. Basic routing protocols, flooding and directed diffusion protocols;
4. Seamless saving of key statistics, which are stored in a *python cPickle* file in the form of the flexible data structure *python hash*;
5. Several different user interfaces.

NECO includes three ways of running simulations: (1) a graphical user interface (GUI), (2) a command-line option and an (3) XML file for simple setup of simulation parameters. The GUI can

be used for easy debugging, visualization of graphs and verification of protocol steps, as shown in *Figure 1*.



The GUI of NECO is divided in three main components. At the left is the control component, in which the simulation parameters can be controlled beforehand, and the simulation output is updated when the simulation is running. The network visualization part is located in the middle; protocols can be easily followed since the links in usage and the ones in which information has been transmitted are highlighted using different colours. An histogram is located at the left, which shows the influence of the topology in network coding protocols.

The setup of simulation parameters can also be performed through an XML description. This is available both through the GUI and the command line option. It is also possible to save the current simulation parameters to a new XML file.

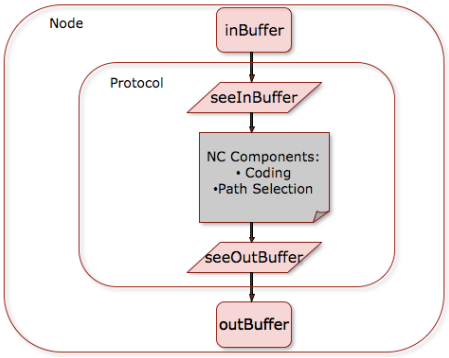
Statistics

NECO contains methods for saving important statistics, which can be found in the *Statistics* class. The *Statistics* class contains two main methods: *writeConstant* and *writeTimeDependent*. The first one can be used to save constant information, such as constant graph parameters or simulation seeds. The second one can be used to save variables that change over time such as, for example, the number of packets that each node received at each simulation step.

Network and protocol abstractions

Since our main focus is on the simulation of protocols for complex networks, we abstract from the network stack and implement a simplified version produced specifically for network coding protocols, which is shown in *Figure 2*. The incoming and outgoing links are represented by two buffers – the *inBuffer* and the *outBuffer*, respectively. Network coding protocol implementations simply check the *inBuffer* for received packets, the packets undergo processing in the main NC components, that is, coding and path selection, and proceed to the *outBuffer*.

In order to save processing time in simulating network coding protocols, we exploit the fact that all quantities of interest can



A simplified stack for network coding protocol testing.

be either directly measured or computed from the encoding matrices present at each node, and focus entirely on the encoding vectors [2, 4] of each packet, that is, the payload of the packets is not included in the simulation.

Conclusion

We presented an open-source network coding simulator which features a high performance and easily extensible core. Our long-term plans include the addition of more graph models, such as evolving networks for evaluation of distributed storage, peer to peer models and mobility models.

Version 1.0 of NECO was released on March, 20th 2009 and is available for download at http://www.dcc.fc.up.pt/∼neco.

Bibliography

[1] R. Ahlswede, N. Cai, S. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[2] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, October 2004.

[3] D. Lun, M. Médard, R. Koetter, and M. Effros, "Further results on coding for reliable communication over packet networks," *IEEE International Symposium on Information Theory (ISIT)*, pp. 1848–1852, 2005.

[4] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, 2003.

Delay Constrained Network Coding

Rui A. Costa, Maricica Nistor, Fausto Vieira, João Barros

The issue of delay between data transmission and successful delivery to the receiving application is arguably one of the key concerns when applying coding ideas to networking problems. This is particularly true for network coding, where nodes combine multiple packets by means of algebraic operations and perform computationally heavy Gaussian elimination algorithms to recover the sent data. Although there is growing consensus that in wireless broadcast scenarios network coding can bring benefits in terms of throughput and robustness, the fact that a receiver may have to wait for a considerable number of packets before it can decode the data, justifies the question whether and how network coding can be used in scenarios with stringent end-to-end delays.

In the seminal paper of Ahlswede, Cai, Li, and Yeung, which shows that network coding is required to achieve the multicast capacity of a general network, the problem is formulated in an information-theoretic setting, where delay and complexity are not taken into account. Delay is also not a primary concern of the algebraic framework of the random linear network coding method, in which each node in the network randomly selects a set of coefficients and uses them to form linear combinations of the data symbols (or packets) it receives. When intermediate nodes cannot perform coding operations and applications are able to tolerate some delay, fountain codes (e.g., Raptor codes) emerge as a viable solution offering low coding overhead as well as near-optimal throughput over packet erasure channels.

Clearly, in all of these instances, coding is performed in a feedforward fashion. The encoders upstream are oblivious to packet loss downstream and their coding decisions do not exploit any feedback information. In contrast, the Delay Constrained Network Coding property that transmitted packets are linear combinations of subsets of packets available at the sender buffer, suggests that network coding protocols could be enhanced by modifying the content of the acknowledgments typically provided by transport protocols. Instead of acknowledging specific packets, each destination node of a unicast or multicast session can send back requests for degrees of freedom that increase the dimension of its vector space and allow for faster decoding.

Recent contributions that pursue this idea (e.g., [1]) focus mostly on end-to-end reliability with perfect feedback, i.e., complete and immediate knowledge of the packets stored at each receiver. The source node reacts by sending the most innovative linear combination that is useful to most destination nodes. Throughput optimal network coding protocols following this concept appear in [2], which introduce the useful notion of *seen* packet as an abstraction for the case in which a packet cannot yet be decoded but can be safely removed from the sender buffer. Removing packets in a timely fashion has obvious benefits in terms of queue length. By using the feedback information to move a *coding window* along the sender buffer instead of mixing fixed sets of packets (also called generations), these protocols perform *online* network coding in the sense that they adapt their coding decisions based on the erasure patterns observed in the network.

Realizing that existing solutions do not yet cover the full range of trade-offs between throughput and delay, in particular when users experience different packet loss probabilities, we set out to provide end-to-end delay control for online network coding with feedback. In [3], we provide the following contributions:

- *Delay Analysis:* We provide an analytical framework to evaluate the delay performance of online network coding algorithms that leverage feedback for increased reliability. The novelty of our approach lies in observing how each erasure event affects the chains of undecoded linear combinations that build up at the receiver buffer. Moreover, we can map the information backlog between receivers to an appropriate random walk on a high dimensional lattice, which brings further insight into the delay behavior.
- *Online Network Coding Algorithms with Delay Constraints:* Using the knowledge of the chain length at each receiver, we identify simple ways of limiting the delay by means of informed encoding decisions. In particular, we show the benefits of sending uncoded packets to alleviate the delay of weaker receivers.

Example of Online Network Coding with ARQ

Time Slot	Sent Packet	Receiver 1	Receiver 2
1	$\mathbf{p_1}$	OK	E
2	$\mathbf{p_1} \oplus \mathbf{p_2}$	OK	OK
3	$\mathbf{p_2} \oplus \mathbf{p_3}$	OK	OK
4	$\mathbf{p_3} \oplus \mathbf{p_4}$	OK	OK
5	$\mathbf{p_4} \oplus \mathbf{p_5}$	OK	E
6	$\mathbf{p_4} \oplus \mathbf{p_6}$	OK	OK
7	$\mathbf{p_6} \oplus \mathbf{p_7}$	E	OK
8	$\mathbf{p_7}$	OK	OK
9	$\mathbf{p_5} \oplus \mathbf{p_8}$	OK	OK
10	$\mathbf{p_8} \oplus \mathbf{p_9}$	E	OK
11	$\mathbf{p_9}$	OK	E
12	$\mathbf{p_9} \oplus \mathbf{p_{10}}$	OK	OK

Example of Systematic Online Network Coding

Time Slot	Sent Packet	Receiver 1	Receiver 2
1	$\mathbf{p_1}$	OK	*E*
2	$\mathbf{p_2}$	OK	OK
3	$\mathbf{p_3}$	OK	OK
4	$\mathbf{p_4}$	OK	OK
5	$\mathbf{p_5}$	OK	*E*
6	$\mathbf{p_6}$	OK	OK
7	$\mathbf{p_7}$	*E*	OK
8	$\mathbf{p_1} \oplus \mathbf{p_7}$	OK	OK
9	$\mathbf{p_8}$	OK	OK
10	$\mathbf{p_9}$	E	OK
11	$\mathbf{p_5} \oplus \mathbf{p_9}$	OK	E
12	$\mathbf{p_{10}}$	OK	OK

Our work differs from [2] in that we consider heterogeneous users with different erasure probabilities and take the end-to-end delay to be our main figure of merit. Also centered around equal erasure probabilities for all users, the contribution in [4] focuses on the two user case and uses only the binary field, whereas, in contrast also with [1], we consider also larger field sizes and larger number of users. A different method to limit the delay is to mix packets in such a way that at least some of the receivers are able to decode a symbol immediately upon receiving a new packet. If no feedback information is available, the best one can do is to choose the packets randomly and optimize only the number of packets to be combined, an approach which appears adequate for highly constrained scenarios such as data preservation in sensor networks. Results on the optimum degree distributions with respect to network dynamics and topology can be found in [5]. The use of feedback under similar assumptions was explored in [6]. We believe that our algorithms are able to reach a larger set of operating points in the delay-throughput plane and are thus well suited for streaming applications with stringent delay requirements, where network coding has already proved to yield competitive solutions.

Bibliography

[1] L. Keller, E. Drinea, and C. Fragouli, "Online broadcasting with network coding," in *NetCod*, Hong Kong, China, Jan. 2008.

[2] J. K. Sundararajan, D. Shah, and M. Medard, "ARQ for network coding," in *IEEE ISIT 2008*, Toronto, Canada, Jul. 2008.

[3] J. Barros and R. A. Costa and D. Munaretto and J. Widmer, "Effective Delay Control in Online Network Coding", *Proc. IEEE Conference on Computer Communications (Infocom)*, Atlanta (GA), USA, April 2009.

[4] J. Sundararajan, D. Shah, and M. Médard, "Online network coding for optimal throughput and delay–the two-receiver case," *Arxiv preprint arXiv:0806.4264*, 2008.

[5] D. Munaretto, J. Widmer, M. Rossi, and M. Zorzi, "Resilient Coding Algorithms for Sensor Network Data Persistence," in *EWSN*, Bologna, Italy, Jan. 2008.

[6] R. A. Costa, D. Munaretto, J. Widmer, and J. Barros, "Informed network coding for minimum decoding delay," in *IEEE MASS*, Atlanta, Georgia, Sep. 2008.

Lightweight Security for Network Coding

João P. Vilela, Luísa Lima, and João Barros

Under the emerging network coding paradigm, intermediate nodes in the network are allowed not only to store and forward packets but also to process and mix different data flows. We propose a low-complexity cryptographic scheme that exploits the inherent security provided by random linear network coding and offers the advantage of reduced overhead in comparison to traditional end-to-end encryption of the entire data. Confidentiality is achieved by protecting (or "locking") the source coefficients required to decode the encoded data, without preventing intermediate nodes from running their standard network coding operations.

Introduction

Since the seminal paper of Ahlswede, Li, Cai and Yeung [1], where it is proved that the maximum capacity of a general multicast network can only be achieved by allowing intermediate nodes to mix different data flows, a surge in *network coding* research has uncovered its potential to provide higher throughput and robustness.

Random Linear Network Coding (RLNC) is a distributed methodology for performing network coding, in which each node in the network independently and randomly selects a set of coefficients and uses them to form linear combinations of the data packets it receives. Each packet is sent along with a global encoding vector, which is the set of linear transformations that the original packet goes through on its path from the source to the destination. The global encoding vector enables the receivers to decode the original data using Gaussian elimination.

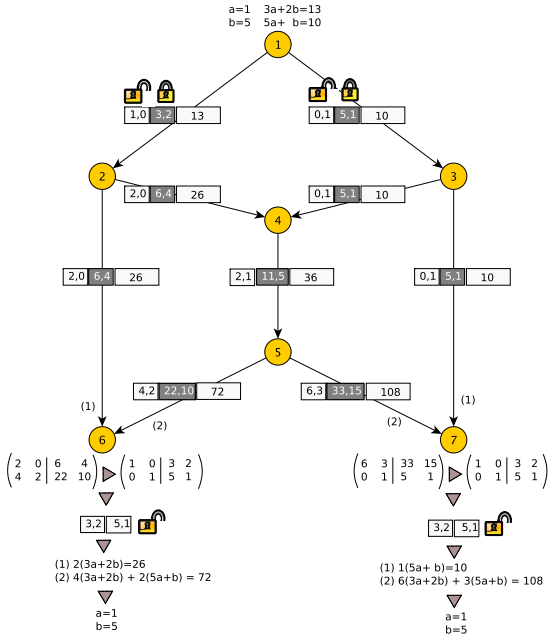
When it comes to security, current proposals are mainly of a theoretical nature and focus on a limited attacker. In particular, a set of coding schemes have been proposed to tackle an eavesdropper with access to a limited number of links of the network.

Motivated by the security challenges of emerging network coded systems we present a lightweight cryptographic scheme to ensure confidentiality in network coding, which leverages the inherent security provided by RLNC to reduce the overhead in comparison to end-to-end encryption of the entire data flow. The main novelty of our approach lies in protecting (or "locking") the source coefficients required to decode the linearly coded data, while still allowing intermediate nodes to carry out the usual network coding operations on a set of coefficients containing the "unlocked" coefficients followed by the "locked" coefficients.
Thus, our security mechanisms can be combined with state-of-the-art network coding protocols without the need to modify the coding procedures at the intermediate nodes.

Lightweight Security for Network Coding

We propose SPOC (Secure Practical Network Coding) [2], a security framework that exploits the interplay between the intrinsic security of network coding and standard cryptographic mechanisms with the goal of countering a full-fledged attacker, which can observe every transmission in the network.
We define two types of coefficients: (1) the *unlocked coefficients*, which are basically a line of coefficients drawn from the identity matrix for each coded packet, and (2) the *locked coefficients*, which are actually used for encoding and decoding yet are encrypted with keys that are shared with the destination nodes. The unlocked and locked coefficients are concatenated and added to the packet header whenever a new packet is generated, thus forming the global encoding vector.
The full set of coefficients (locked and unlocked) is processed by the intermediate nodes following the exact same packet mixing rules of the original RLNC based protocol.
To illustrate the basic principles of the proposed scheme, *Figure 1* presents the canonical network coding example with the modifications introduced by our approach. The operations in this example can be described as follows.

1. The *source node 1* randomly generates the locked coefficients and encrypts them with the keys shared with the sink nodes *6* and *7* using one of the already mentioned cryptosystems. The unlocked coefficients of each packet are simply distinct lines of the identity matrix which allow subsequent nodes to check if the packets are linearly independent or not, and carry out the protocol using this information;
2. The subsequent *intermediate nodes* perform the usual combination of packets (e.g. node *4* combines the packets received from nodes *2* and *3* using the $(1,1)$ encoding vector). The intermediate nodes do not differentiate between



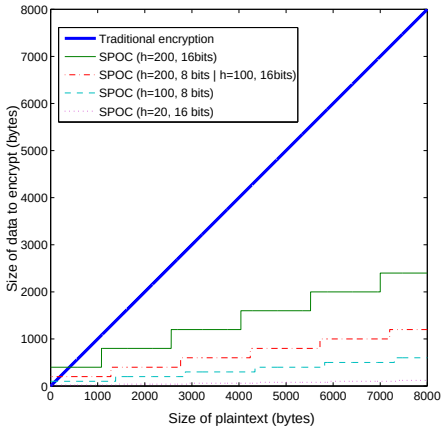
Basic scheme. White parts of packets represent clear-text information, whereas encrypted information is shaded in grey. In practice, the initial locked coefficients in grey – (3,2) and (5,1) – are encrypted to other symbols of the same size. For illustration purposes, the scheme is simplified using integers.

the locked and unlocked coefficients, in that they perform exactly the same operations on both;

3. When sufficient information reaches the *destination nodes 6* and *7*, they recover the original locked coefficients using the knowledge of the transformation they suffered – available through the unlocked coefficients. Then, they decrypt the locked coefficients and compute the product with the unlocked coefficients. The destination nodes finally perform Gaussian elimination to recover the native packets.

Performance Gains

To illustrate SPOC's efficiency in comparison to traditional end-to-end encryption, *Figure 2* compares the volume of data to be encrypted according to the size of the plaintext. We consider a maximum payload size of 1480 bytes (a typical value e.g. for the Ethernet) and assume that at each point in time, SPOC has h packets to code. In the case of the traditional encryption mechanism, which performs end-to-end encryption of the entire payload, the volume of data that must be encrypted increases linearly with the size of the protected payload. It is not difficult to see that, by encrypting solely the locked coefficients, SPOC substantially reduces the size of information to be encrypted (both in the case of 8 bit and 16 bit coefficients), while still guaranteeing strong confidentiality of the payload.



Size of data to be encrypted, for SPOC (encryption of locked coefficients) versus traditional encryption (encryption of the whole data).

Conclusion

We presented a security scheme that assures confidentiality in network coding protocols based on the interplay between the coding properties in this paradigm and cryptographic mechanisms. Specifically, we attained a substantial reduction on the size of the data to be encrypted when compared to the naïve encryption approach (where the whole data needs to be encrypted) and, consequently, a reduction of the computational overhead required to perform encryption. Confidentiality is achieved by protecting (or "locking") the source coefficients required to decode the linearly coded data, and by letting intermediate nodes run their operations on a set of coefficients composed by the "unlocked" and the "locked" coefficients that do not impair any of the operations of practical network coding protocols. Follow-up work which (1) characterizes the correlation between the encoded data and the two elements that can lead to information disclosure – the source coefficients and the original data itself – and (2) proposes improved coding schemes, is available in [3].

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *Information Theory, IEEE Transactions on*, vol. 46, no. 4, pp. 1204–1216, Jul 2000.

[2] J. P. Vilela, L. Lima, and J. Barros, "Lightweight Security for Network Coding," *Proc. of the IEEE International Conference on Communications (ICC 2008), Beijing, China*, May 2008.

[3] L. Lima, J. P. Vilela, J. Barros, and M. Médard, "An Information-Theoretic Cryptanalysis of Network Coding – is Protecting the Code Enough?" *International Symposium on Information Theory and its Applications (ISITA 2008), Auckland, New Zealand*, December 2008.

Byzantine Attacks against Network Coding in P2P Distributed Storage

Luísa Lima and João Barros

We consider the impact of Byzantine attackers on peer-to-peer topologies for distributed storage using network coding. First, the problem is formulated as one of data flow in random evolving graphs, in which a data source and a data collector are connected to data keepers who may behave in a Byzantine fashion. We then derive analytical results for the probability of carrying out a successful distributed denial of service attack (that is, collecting contaminated information from the network), as well as the expected number of contaminated nodes at each timestep. Our results show that, even for a small number of Byzantine attackers in the network, the probability of collecting contaminated information is overwhelming, and that the dissemination of information by peers as opposed to a selected subset of nodes in the network increases the probability of contaminated information collection.

Introduction

Under the classical networking paradigm, in which intermediate nodes are only allowed to store and forward packets, information security is usually viewed as an independent feature with little or no relation to other communication tasks. As a distributed capacity-achieving approach for the multicast case, Random Linear Network Coding (RLNC) [1] has been shown not only to provide an intrinsic level of data confidentiality, but also to extend naturally to packet networks with losses, and, simultaneously, to provide increased resilience against failures in the network.

In RLNC based protocols, each node in the network independently and randomly selects a set of coefficients and uses them to form linear combinations of the data symbols it receives. Each symbol or packet is sent along with the global encoding vector, which, provided that the received matrix has full rank, enables the receivers to decode the original data using Gaussian elimination.

The inherent robustness properties of RLNC make it particularly suitable as a framework for dynamic and unstable networks, such as delay tolerant networks and content distribution networks. In particular, its operation is completely desynchronized and local, since each node forwards a random linear combination independently of the information present at other nodes. Additionally, when collecting a random combination of packets, there is a high probability of getting a linearly independent packet, and thus, the problem of redundancy caused by traditional flooding approaches is diluted, since there is no need to download one particular fragment; instead, any linearly independent fragment is likely to bring innovative information [2].

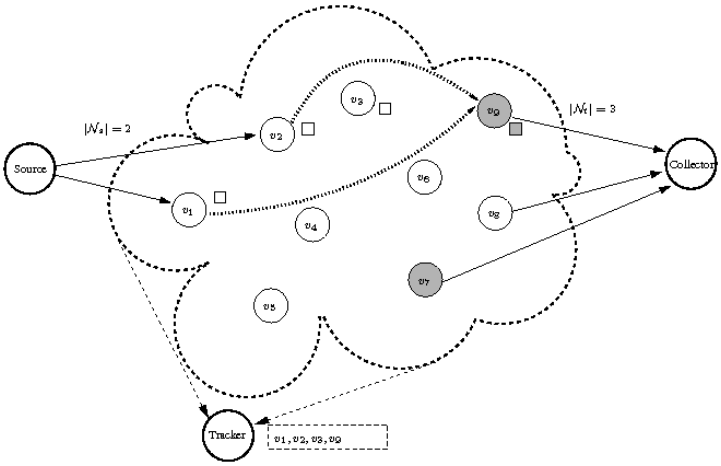
In spite of having desirable properties for several distributed networking settings, RLNC is particularly susceptible to *Byzantine attacks*, that is, the injection of corrupted packets into the information flow. Since network coding relies on mixing the content of multiple data packets, a single corrupted packet may very easily corrupt the entire information flow from the sender to the destination at any given time [3, 4]. Previous work regarding this issue has focused both on the detection and correction of Byzantine modifications in data flow networks [3, 4]. Active attacks can be particularly disruptive in peer to peer content distribution networks. In fact, in this kind of networks, there is typically no security control over the nodes that join the network and the blocks that they redistribute. Additionally, the topologies of the overlay graphs that arise from traditional peer to peer connection models are typically scale-free and small-world networks, which have been shown to be especially prone to the dissemination of epidemics, such as worms and viruses.

Motivated by these observations, we set out to evaluate the potential impact of multiple Byzantine attackers in peer to peer distributed storage networks. First, we formulate the problem as one of data flow in random evolving graphs, in which a source and a collector are connected to an evolving random network of data keepers which may become Byzantine with a certain probability. Then, we propose a methodology for evaluating the impact of Byzantine attacks in peer-to-peer distributed storage networks. Finally, we derive analytical bounds for the expected number of contaminated nodes and for the probability of collecting contaminated information from the data keeper network.

Even for a small number of Byzantine attackers in the network, the probability of collecting contaminated information in peer-to-peer networks with network coding is overwhelming.

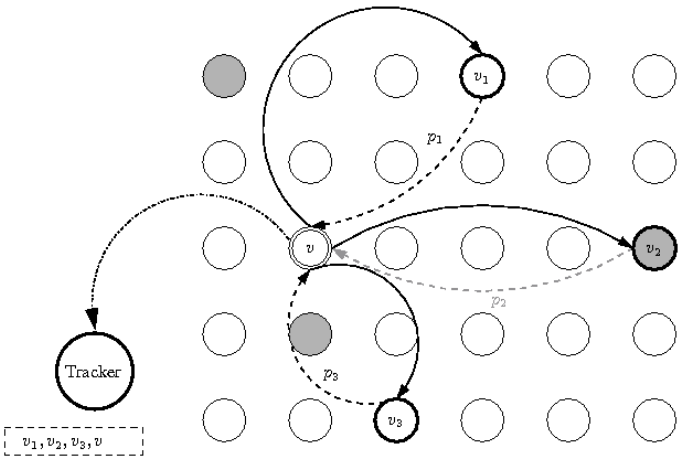
Model

We consider three types of nodes: a data *source*, a data *collector* and data *keepers*. Each keeper stores one packet, which is coded according to the rules of RLNC. The data source and the data collector only connect to the data keepers, and the data collector attempts to retrieve stored data packets after a certain time. Although both the data source and the data collector are assumed to be honest, each keeper has a certain probability of becoming Byzantine. A scheme of the network is represented in *Figure 1*.



Network Model. Data keepers are represented by the nodes inside the network cloud; packets are represented by squares. Grey nodes represent Byzantine nodes. The tracker is represented by the node outside of the network, with the list of informed nodes on its right.

The keepers are disconnected in the beginning of the evolution process. We consider an evolving graph representing the contacts between keeper nodes in the network. At each timestep, one of the data keepers that are connected to the data collector asks the tracker for a set of nodes storing one packet. The tracker returns a random list of these nodes, to which the requesting keeper connects directly (in a secure overlay network fashion). Each node in the set node communicates its stored packet using a direct link connection as well. Afterwards, the keeper stores a random linear combination of the packets sent. The process is repeated for all data keepers that are connected to the data collector.
A schematic representation of the process is represented in *Figure 2*.



Dissemination model. At each timestep, a new keeper node requests a packet from a subset of nodes in the list provided by the tracker. The keeper stores contaminated information if it is Byzantine itself or connects to a contaminated node.

Results

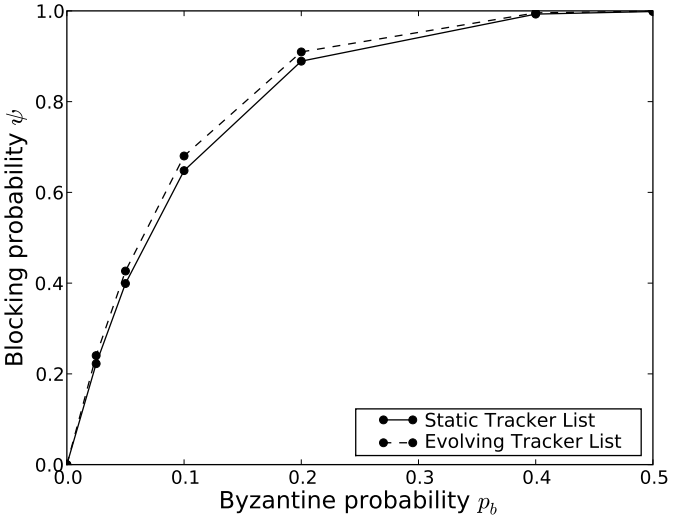
To illustrate the difference between a peer-to-peer network and a traditional distributed storage network, we consider two cases for the list of nodes kept at the tracker:

1. A static case in which the tracker only keeps a list of the nodes that are directly connected to the source and does not update it during the information dissemination process;
2. An evolving case in which the tracker updates the list with each new node storing a packet.

The results for the probability of collecting contaminated information (that is, the blocking probability) are shown in *Figure 3*; it grows exponentially for both cases considered. The growth is faster for the evolving case. In fact, as more nodes are added to the network, the presence of contaminated keepers becomes more likely, and thus, the probability that a new node is connected to one or more contaminated keepers increases.

Conclusions

We used randomly evolving graphs to characterize the impact of Byzantine attackers on peer-to-peer topologies for distributed storage. Our results show that the dissemination of information by peers, as opposed to a selected subset of nodes in the network, increases the probability of collecting contaminated information and that the probability of this DDoS attack is overwhelming even for a small number of Byzantine nodes in the network. As part of our ongoing work, we are evaluating how the rules of preferential attachment [5] can be leveraged for robust distributed storage.



Blocking probability in function of the number of Byzantine nodes in the network for 30 data keepers, 5 of which are connected to the source and 6 to the collector. The results for the static and evolving list at the tracker are shown in full and dashed, respectively.

Acknowledgements

Joint work with Ralf Koetter (Institute for Communications Engineering of the Technischen Universitaet Muenchen, Germany)

Bibliography

[1] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[2] A. G. Dimakis, P. B. Godfrey, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," in *IEEE INFOCOM 2007, Anchorage, Alaska, USA*, May 2007. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:cs/0702015

[3] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient Network Coding In the Presence of Byzantine Adversaries," in *IEEE INFOCOM 2007. 26th IEEE International Conference on Computer Communications, Anchorage, Alaska, USA*, May 2007.

[4] C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in *IEEE Infocom, Barcelona, Spain*, April 2006.

[5] A. Barabási and R. Albert, "Emergence of Scaling in Random Networks," *Science*, vol. 286, no. 5439, p. 509, 1999.

A Network Coding Approach to Secret Key Distribution

Paulo F. Oliveira and João Barros

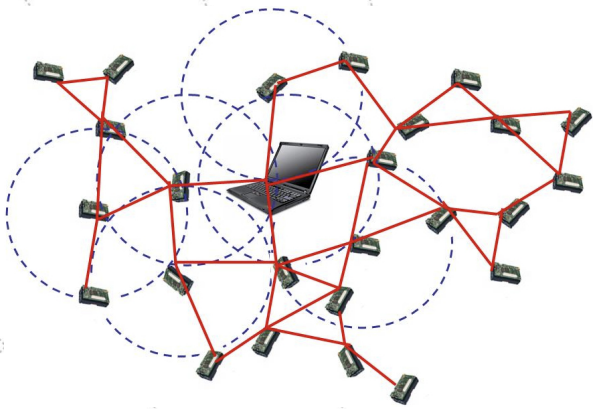
We consider the problem of secret key distribution in a sensor network with multiple scattered sensor nodes and a mobile device that can be used to bootstrap the network. Our main contribution is a set of secure protocols that rely on simple network coding operations to provide a robust and low-complexity solution for sharing secret keys among sensor nodes, including pairwise keys, cluster keys, key revocation, and mobile node authentication. Our results include performance evaluation in terms of security metrics and a detailed analysis of resource utilization. The basic scheme was implemented and tested in a real-life sensor network testbed.

Introduction

The ability to distribute secret keys in a secure manner is an obvious fundamental requirement towards assuring cryptographic security. In the case of highly constrained mobile ad-hoc and sensor networks, key predistribution schemes emerge as a strong candidate, mainly because they require considerably less computation and communication resources than trusted party schemes or public-key infrastructures. The main caveat is that secure connectivity can only be achieved in probabilistic terms, i.e. if each node is loaded with a sufficiently large number of keys drawn at random from a fixed pool, then with high probability it will share at least one key with each one of its neighboring nodes.

We consider the scenario in which a mobile node (e.g., a handheld device or a laptop computer) is available for bootstrapping the network and is used to help establish secure connections between the sensor nodes. In contrast with pure key predistribution schemes, we propose the combined use of network coding and mobility and show how these tools can be used effectively to establish secure connections between sensor nodes [1], offering the following advantages:

- *Deterministic Security*: The use of a mobile node ensures that links are secured with probability one.
- *Global Efficiency*: in addition to a small number of transmissions and low-complexity processing (mainly XOR operations), each node is required to prestore only a small number of keys (as many as its expected number of links).



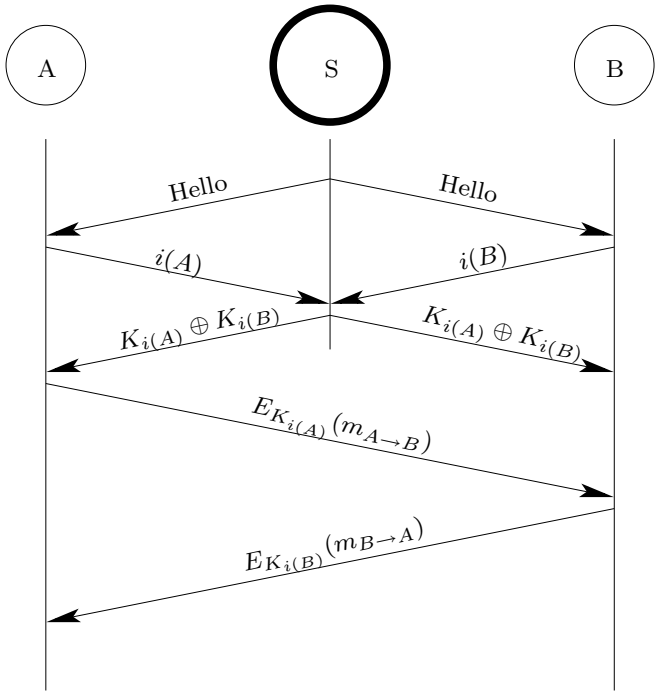
A wireless sensor network is a collection of small devices that, once deployed on a target area, organize themselves in an ad-hoc network, collect measurements of a physical process and transmit the data over the wireless medium to a data fusion center for further processing. If a mobile node (represented here by a laptop computer) is available, then it can be used to establish secure links between sensor nodes.

- *"Blind" Key Distribution*: although the mobile node only sees encrypted versions of the secret keys, it is capable of using network coding to ensure that each pair of sensor nodes receives enough data to agree on a pair of secret keys.

Mobile Secret Key Distribution Scheme

The basic scheme performed prior to sensor node deployment can be summarized in the following tasks:

1. a large pool P of N keys and their N identifiers are generated off-line;
2. a different subset of L keys drawn randomly from P and the corresponding L identifiers are loaded into the memory of each sensor node;
3. a table is constructed with the N key identifiers and N sequences that result from performing an XOR of each key with a common protection sequence X;
4. the table is stored in the memory of the mobile node.



Secret key distribution protocol after sensor node deployment. Sensor nodes *A* and *B* want to exchange two keys via a mobile node *S*. The process is initiated by a HELLO message broadcast by *S*. Upon receiving this message, each sensor node sends back a key identifier corresponding to one of its keys. Based on the received key identifiers, *S* locates the corresponding sequences protected by *X* and combines them through an XOR network coding operation, thus canceling *X*, and broadcasts the resulting XOR sequence. By combining the received combination with its own key, each node can easily recover the key of its neighbor node, thus sharing a pair of keys which is kept secret from the mobile node. After recovering each other's keys by simple XOR operations, the nodes communicate securely by encrypting their messages.

By exploiting the benefits of network coding and mobility, it is possible to design an efficient secret key distribution scheme in which the mobile node is provably oblivious to the distributed keys.

In addition to the basic key distribution scheme, we also include a specific collection of relevant extensions as follows [2, 3]:

- *Key Renewal for Robustness and Scalability in Dynamic Environments*: if the network topology changes rapidly, new keys can be safely distributed with a simple procedure even when the sets of prestored keys have been depleted.
- *Authentication, Clustering and Key Revocation*: we provide additional protocols that cover authentication of the mobile node, generation of cluster keys, and revocation in the case of compromised sensor nodes.
- *Performance Evaluation*: we provide a thorough analysis of the security performance of our scheme by discussing its behavior under various attack models and proving mathematically that the encrypted keys stored by the mobile node are information-theoretically secure.
- *Implementation and Testing*: as a proof-of-concept, we implemented and tested the basic XOR-based key distribution scheme on TelosB motes, running the TinyOS 2.0 operating system.

Conclusion

We presented a secret key distribution scheme for large sensor networks. In contrast with pure key predistribution schemes, any two nodes that can reach each other can communicate securely with probability one, using a small number of pre-stored keys albeit at the expense of a mobile node for bootstrapping. Since our protocol and its extensions can easily accommodate for additional nodes, new keys and secured links, we deem the proposed network coding approach to be well suited for dynamic sensor networks with stringent memory and processing restrictions. We believe that some of the proposed techniques will find natural applications also in other classes of mobile ad-hoc networks composed of devices with limited processing and transmission capabilities.

Although our use of network coding was so far limited to XOR operations, using linear combinations of symbols is likely to yield more powerful schemes for secret key distribution. Thus, part of our ongoing work is devoted to exploiting random linear network coding [4] and extending these ideas to multi-hop secret key distribution in highly dynamic networks.

Bibliography

[1] P. F. Oliveira, R. A. Costa, and J. Barros, "Mobile Secret Key Distribution with Network Coding," in *Proc. of the International Conference on Security and Cryptography (SECRYPT)*, July 2007.

[2] P. F. Oliveira and J. Barros, "Network Coding Protocols for Secret Key Distribution," in *Proc. of the International Symposium on Information Security (IS'07)*, November 2007.

[3] ——, "A Network Coding Approach to Secret Key Distribution," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 414–423, 2008.

[4] L. Lima, M. Médard, and J. Barros, "Random Linear Network Coding: A Free Cipher?" in *Proc. of the IEEE International Symposium on Information Theory (ISIT)*, June 2007.

Capacity of Random Networks

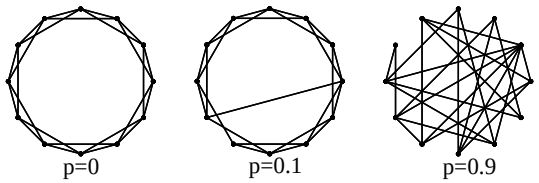
Rui A. Costa and João Barros

In the quest for the fundamental limits of communication networks, whose topology is typically described by graphs, the connection between the maximum information flow and the minimum cut of the network plays a singular and prominent role. In the case where the network has one or more independent sources of information but only one sink, it is known that the transmitted information behaves like *water in pipes* and the capacity can be obtained by classical network flow methods. Specifically, the capacity of this network will then follow from the well-known Ford-Fulkerson *max-flow min-cut* theorem [1], which asserts that the maximal amount of a flow (provided by the network) is equal to the capacity of a minimal cut, i.e. a nontrivial partition of the graph node set V into two parts such that the sum of the capacities of the edges connecting the two parts (the cut capacity) is minimum. Provided there is only a single sink, routing offers an optimal solution for transporting messages both when they are statistically independent and when they are generated by correlated sources [2].

Max-flow min-cut arguments are useful also in the case of multicast networks, in which a single source broadcasts a number of messages to a set of sinks. This network capacity problem was solved in [3], where it is shown that applying coding operations at intermediate nodes (i.e. *network coding*) is necessary to achieve the max-flow/min-cut bound of a general network. A converse proof for this problem, known as the *network information flow problem*, was provided by [4].

When the topology of the network is modeled by a randomly constructed graph, the natural goal is a probabilistic characterization of the minimum cut, which in the spirit of the network information flow literature [3] we call the *capacity* of the random network. Although some capacity results of this flavor are available for particular instances, the problem remains open for many relevant classes of random graphs. Motivated by this observation, our contributions (with some parts presented in [5], [6] and [7]) are as follows:

- *A Max-flow Min-cut Theorem:* We introduced the *independence-in-cut* property, which is satisfied by large classes of random graphs, and derived inner and outer bounds for the minimum cut of any network that possesses this basic property.
- *Capacity Bounds for Small-World Networks:* Based on the aforementioned max-flow min-cut theorem, we were able to characterize the max-flow min-cut capacity of Small-World networks with shortcuts and with rewiring [8]. Our results show, somewhat surprisingly, that, up to a constant factor, a rewiring rule that preserves the independence-in-cut property does not affect the capacity of large small-world networks.
- *Capacity Bounds for Dual Radio Networks:* We are able to apply our theorem also to wireless network models in which some of the nodes are able to establish both short-range and long-range connections by means of dual radio interfaces. The capacity bounds obtained show that the capacity of dual radio networks grows quadratically with the fraction of dual radio devices, thus indicating that a small percentage of such devices is sufficient to improve significantly the maximum information flow in the network.



Small-world model with rewiring for different values of the rewiring probability p.

Our motivation to consider small-world networks, i.e. graphs with high clustering coefficients and small average path length, stems from their proven ability to capture fundamental properties of relevant phenomena and structures in sociology, biology, statistical physics and man-made networks. Beyond well-known examples such as Milgram's "six degrees of separation" between

any two people in the United States and the Hollywood graph with links between actors, small-world structures appear in such diverse networks as the U.S. electric power grid, the nervous system of the nematode worm *Caenorhabditis elegans*, food webs, telephone call graphs, and, most strikingly, the World Wide Web.

The term small-world graph itself was coined by Watts and Strogatz, who in their seminal paper [8] defined a class of models which interpolate between regular lattices and random Erdös-Rényi graphs by adding shortcuts or rewiring edges with a certain probability p. The most striking feature of these models is that for increasing values of p the average shortest-path length diminishes sharply, whereas the clustering coefficient, defined as the expected value of the number of links between the neighbors of a node divided by the total number of links that could exist between them, remains practically constant during this transition.

Since small-world graphs were first proposed as models for complex networks, most contributions have focused essentially on connectivity parameters such as the degree distribution, the clustering coefficient or the shortest path length between two nodes. In spite of its arguable relevance — particularly where communication networks are concerned — the *capacity* of small-world networks was, to the best of our knowledge, not studied in depth by the scientific community until our first publication on this topic.

With respect to Dual Radio Networks, our research is motivated by the fact that wireless interfaces become standard commodities and communication devices with multiple radio interfaces appear in various products. Thus, it is only natural to ask whether the aforementioned devices can lead to substantial performance gains in wireless communication networks. Promising examples include the use of multiple radios to provide better performance and greater functionality for users, and field experiments where it is shown that using radio hierarchies can reduce power consumption. This growing interest in wireless systems with multiple radios (for example, a Bluetooth interface and an IEEE 802.11 wi-fi card) motivate us to study the impact of dual radio devices on the capacity of wireless networks.

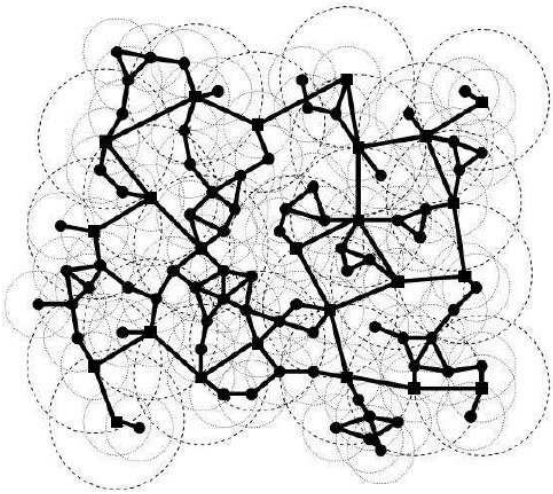


Illustration of Dual Radio Networks: the square nodes represent the devices with two wireless technologies, whereas devices with only one wireless technology are represented by circles; the small and large circumferences represent the coverage area of the short-range and of the long-range wireless interfaces, respectively.

Bibliography

[1] L. Ford and D. Fulkerson, *Flows in Networks*. Princeton University Press, Princeton, NJ, 1962.

[2] J. Barros and S. D. Servetto, "Network information flow with correlated sources," *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 155–170, January 2006.

[3] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[4] S. Borade, "Network information flow: Limits and achievability," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Lausanne, Switzerland, July 2002.

[5] R. A. Costa and J. Barros, "On the capacity of small world networks," in *Proc. of the IEEE Information Theory Workshop*, Punta del Este, Uruguay, March 2006.

[6] ——, "Network information flow in *navigable* small-world networks," in *Proc. of the IEEE Workshop in Network Coding, Theory and Applications*, Boston, MA, USA, April 2006.

[7] ——, "Dual Radio Networks: Capacity and Connectivity," in *Proc. of the 5th International Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (SpaSWiN'07)*, Limassol, Cyprus, April 2007.

[8] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, June 1998.

Analysis, Design and Optimization of Future Communications Systems

Miguel Rodrigues

In the last decade, the advent of the information age has also ignited a revolution in the wireless communications field, to support the ubiquitous access to the Internet at ever increasing information rates. A number of mobile and fixed wireless systems have been gradually introduced, e.g. 2nd and 3rd generation mobile systems as well as WiFi and WiMax, in order to support a large variety of services such as voice, Internet access, etc.

This wireless communications revolution is being fueled by constant technological breakthroughs to enhance transmission performance in wireless settings. For example, major advances that dominated research efforts in the past decade concerned the development of multiple antenna transmission schemes [1,2], as well as the development of powerful error correcting coding schemes, namely turbo codes [3] and low-density parity-check (LDPC) codes [4]. In fact, these powerful techniques are now gradually being incorporated into wireless communications standards and commercial products.

Yet, outstanding open problems still abound in the analysis, design and optimization of key elements of communications systems, e.g., transmit and receive filters. In this context, significant progress has been made in the design of key communications system elements under the standard mean-squared error (MSE) or even the error probability criteria [5-8]. However, considerable less progress has been made in the design of communications system elements under the reliable information transmission rate criterion - the holy grail in communications. The difficulty relates to the fact that close-form mutual information expressions only exist in general for communications systems with Gaussian inputs [9-13]. However, since practical complexity considerations pertaining to the transmission and reception of information dictate the use of discrete inputs (e.g. M-PSK or M-QAM, etc.) rather than the theoretically appealing Gaussian ones, one often has to resort to engineering experience and insight to optimize the system. One classical example relates to the optimization of the information transmission rate of digital subscriber lines (DSL) using the bit loading algorithm [14], which delivers considerable gains though it is non-optimal.

Recently, Guo, Shamai and Verdú have illuminated intimate connections between information theory and estimation theory in a seminal paper [15] (later generalized in follow-up papers [16,17]). In particular, Guo, Shamai and Verdú have shown that in the classical problem of information transmission through the conventional additive white Gaussian noise (AWGN) channel the derivative of the mutual information with respect to the signal-to-noise ratio (SNR) equals the (non-linear) minimum mean-squared error (MMSE), a relationship holding for scalar, vector, discrete-time and continuous-time channels regardless of the input statistics. The relevance of these recent connections derives from the fact that mutual information and MMSE are two canonical operational measures in information theory and estimation theory: mutual information measures the reliable information transmission rate between the input and the output of a system for a specific signaling scheme, while MMSE measures the minimum mean-squared error in estimating the input given the output.

The implications of a framework involving key quantities in information theory and estimation theory are countless both from the theoretical and the more practical perspective. Of particular relevance is the use of the simple connection between the derivative of the mutual information and the nonlinear MMSE to address open problems in the optimization of the reliable information transmission rate of communications systems in innovative manners.

> The interplay between information theory and estimation theory has shown to be very useful in the analysis, design and optimization of communications systems.

This research work has been exploring the intersections between information theory and estimation theory in the analysis, design and optimization of future communications systems. The most relevant research problems include [18]:

- The optimization of linear precoders for multiple-input multiple-output Gaussian channels with arbitrary inputs.

- The optimization of linear precoders for fading multiple-input multiple-output Gaussian channels with arbitrary inputs.

This work represents a collaboration with Prof. Fernando Pérez-Cruz and Prof. Sergio Verdú from Princeton University.

References

[1] V. Tarokh, N. Seshadri and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, pp. 744-765, March 1998.

[2] V. Tarokh, H. Jafarkhani and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Transactions on Information Theory*, vol. 45, pp. 1456-1467, July 1999.

[3] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo codes," *IEEE Transactions on Communication*s, vol. 44, pp. 1261-1271, October 1996.

[4] D. J. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Transactions on Information Theory*, vol. 45, pp. 399-431, March 1999.

[5] D. P. Palomar, J. M. Cioffi, and M. A. Lagunas, "Joint Tx-Rx beamforming design for multicarrier MIMO channels: A unified framework for convex optimization," *IEEE Transactions on Signal Processing*, vol. 51, pp. 2381-2401, September 2003.

[6] A. Scaglione, P. Stoica, S. Barbarossa, G. B. Giannakis, and H. Sampath, "Optimal designs for space-time linear precoders and decoders," *IEEE Transactions on Signal Processing*, vol. 50, pp. 1051-1064, May 2002.

[7] J. Yang and S. Roy, "On joint transmitter and receiver optimization for multiple-input multiple-output (MIMO) transmission systems," *IEEE Transactions on Communications*, vol. 42, pp. 3221-3231, December 1994.

[8] J. Yang and S. Roy, "Joint transmitter-receiver optimization for multiple-input multiple-output systems with decision feedback," *IEEE Transactions on Information Theory*, vol. 40, pp. 1334-1347, September 1994.

[9] W. Yu, W. Rhee, S. Boyd and J. M. Cioffi, "Iterative water-filling for Gaussian vector multiple-access channels," *IEEE Transactions on Information Theory*, vol. 50, pp. 145-152, January 2004.

[10] D. Tse and S. Hanly, "Multiaccess fading channels - Part I: Polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Transactions on Information Theory*, vol. 44, pp. 2796-2815, November 1998.

[11] S. Hanly and D. Tse, "Multiaccess fading channels - Part II: Delay-limited capacities," *IEEE Transactions on Information Theory*, vol. 44, pp. 2816-2831, November 1998.

[12] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels - Part I: Ergodic capacity," *IEEE Transactions on Information Theory*, vol. 47, pp. 1083-1102, March 2001.

[13] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels - Part II: Outage capacity," *IEEE Transactions on Information Theory*, vol. 47, pp. 1103-1127, March 2001.

[14] J. A. C. Bingham, P. S. Chow, and J. M. Cioffi, "A practical discrete multitone transceiver loading algorithm for data transmission over spectrally shaped channels," *IEEE Transactions on Communications*, vol. 43, pp. 773-775, February/March/April 1995.

[15] D. Guo, S. Shamai, and S. Verdú, "Mutual information and minimum mean-square error in Gaussian channels," *IEEE Transactions on Information Theory*, vol. 51, p. 1261-1282, April 2005.

[16] D. P. Palomar and S. Verdú, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Transactions on Information Theory*, vol. 52, pp. 141-154, January 2006.

[17] D. P.Palomar and S. Verdú, "Representation of mutual information via input estimates," *IEEE Transactions on Information Theory*, vol. 53, pp. 453-470, February 2007.

[18] F. Pérez-Cruz, M. R. D. Rodrigues and S. Verdú, "Optimal linear precoding for multiple-input multiple-output Gaussian channels with arbitrary inputs," *IEEE Transactions on Information Theory*, submitted.

Diophantine Codes For Distributed Source Coding

Gerhard Maierbacher and João Barros

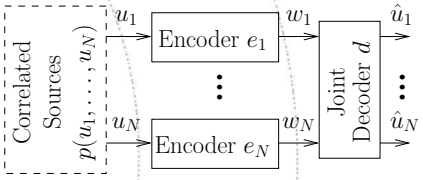
We consider the design of index assignments for the distributed source coding problem in large-scale sensor networks. Using basic tools from number theory, specifically Diophantine analysis, we provide a framework for constructing cyclic index assignments that have very low complexity yet perform very close to fundamental bounds provided by rate-distortion theory.

Introduction and Example

In distributed sensing scenarios, where correlated data has to be gathered by a large number of power-restricted sensors, efficient source coding techniques are key towards reducing the required number of transmissions and enabling extended network life-time. Focusing on low-complexity encoding techniques, we consider distributed scalar quantization (DSQ) of spatially or temporally correlated source observations such that redundancy between source observations is (jointly) removed while each observation (by itself) is encoded separately and independently. The design of distributed quantizers was considered in [1] as well as in previous work [2] based on (heuristic) search algorithms. Our contribution is to provide a constructive framework to exploit the symmetry properties of common source models in order to design low-complexity distributed quantizers.

We consider a system model as depicted in Figure 1 where data from N correlated sources $u_1, u_2, \ldots, u_N$ drawn according to the joint probability distribution $p(u_1, u_2, \ldots, u_N)$ is independently quantized onto (intermediate) indices $i_1, i_2, \ldots, i_N$ and then mapped onto codewords $w_1, w_2, \ldots, w_N$. After error-free transmission the estimates $\hat{u}_1, \hat{u}_2, \ldots, \hat{u}_N$ are formed at the joint decoder, taking advantage of the source correlations. Based on this system setup (distributed) data compression is achieved by choosing index alphabets $I = \{0, 1, \ldots, L-1\}$ of L indices i_n and the codeword alphabets $\mathcal{W}_n = \{s_0, s_1, \ldots, s_{K_n-1}\}$ of K_n codewords w_n, chosen such that $K_n \leq L$, $n = 1, 2, \ldots, N$, i.e. we have less codewords than indices.

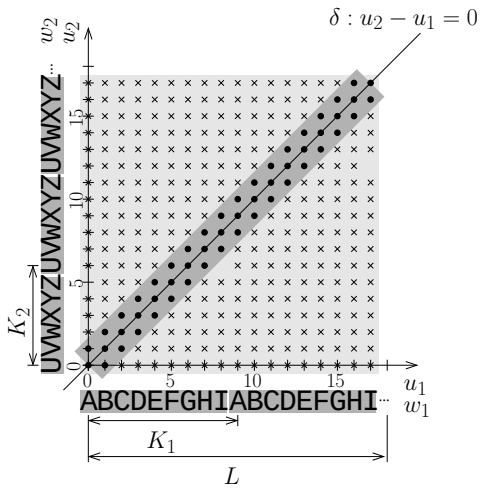
Inspired by insights from fundamental number theory, we consider a simple class of deterministic mapping functions, so called *cyclic index assignments*, and consider the size of the codeword alphabets K_n, $n = 1, 2, \ldots, N$, as the parameter to be optimized.



N correlated sources are independently encoded and jointly decoded. Each transmitter e_n encodes the observed source symbol u_n onto a separate codeword w_n, $n = 1, 2, \ldots, N$. The joint decoder d uses the received codewords $w_1, w_2, \ldots, w_N$ and its knowledge about the source statistics $p(u_1, u_2, \ldots, u_N)$ to jointly form the estimates $\hat{u}_1, \hat{u}_2, \ldots, \hat{u}_N$.

Fundamental properties of distributed source codes based on such mappings can be represented by a set of linear equations whose integral solutions can be found using techniques adopted from Diophantine analysis (a discipline of number theory). Based on those equations, we are able to provide a practical framework for the DSQ design while gaining new insights from the interplay between coding and number theory. For a detailed discussion about the code design and the connection to number theory, please refer to [3].

To gain some intuition, we consider a simple example with two sources, which assumes integer-valued source alphabets $\mathcal{U} = I$ and $L = 18$ indices, see Figure 2. The goal is to construct cyclic index assignments with integer $K_1 \leq \frac{L}{f}$ and integer $K_2 \leq \frac{L}{f}$, in order to reduce the rate from $R_s = \lceil \log_2 L \rceil$ bit per index to $R = \lceil \log_2 \frac{L}{f} \rceil$ bit per codeword. By exploiting the properties of the integer numbers L, K_1 and K_2 themselves, it can be shown that for $L = 18$ and $f = 2$ choosing $K_1 = 9$ and $K_2 = 6$ leads to codes with favorable properties, as illustrated in Figure 2. Specifically it is worth pointing out that all symbol pairs (u_1, u_2) lying within the shaded area around the line $\delta: \; u_2 - u_1 = 0$ are mapped onto different codeword pairs (w_1, w_2), i.e. there are no duplicate codeword pairs within the shaded area. Assuming that only symbol pairs within the shaded area are likely to be generated by the source (e.g. because of strong correlation between u_1 and u_2) then the decoder can reconstruct the original symbol pairs from the received codeword pairs most of the time without error. It is worth mentioning that the shaded area around the line $\delta: \; u_2 - u_1 = 0$ contains exactly those symbol pairs which are the most probable ones for large classes of source models (e.g. bivariate Gaussian



Example for cyclic index assignments. The source symbols u_1, u_2, with $u_1 \in \mathcal{U}$, $u_2 \in \mathcal{U}$, $\mathcal{U} = I$, $I = \{0,1,\ldots,17\}$, are mapped in a cyclic fashion onto the codewords w_1, w_2, with $w_1 \in \mathcal{W}_1$, $\mathcal{W}_1 = \{A,B,C,D,E,F,G,H,I\}$, and $w_2 \in \mathcal{W}_2$, $\mathcal{W}_2 = \{U,V,W,X,Y,Z\}$. Codeword pairs located at the positions indicated by dots reappear only at the positions indicated by crosses. Within the shaded area area around the line $\delta: u_2 - u_1 = 0$ there are no duplicate codeword pairs.

source with subsequent quantization).

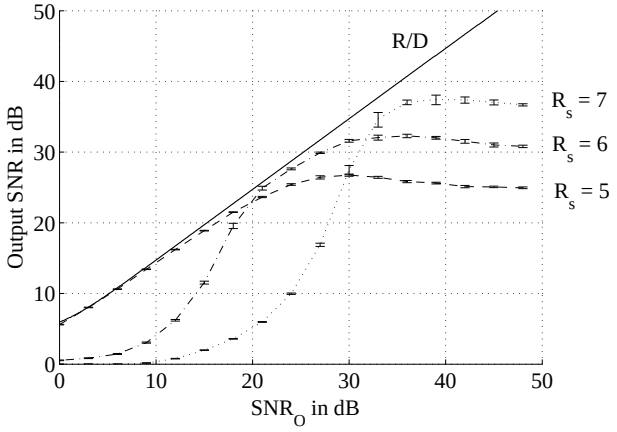
Results and Discussion

To underline the effectiveness and efficiency of our low-complexity coding strategy, we present numerical performance results for the quadratic Gaussian CEO Problem [4].

Let u_0 be the output of a continuous-valued Gaussian source U_0. For $n = 1,2,...,N$, let u_n denote noisy observations of u_0 corrupted by additive noise samples such that $u_n = u_0 + n_n$ where the noise samples n_n are generated by Gaussian noise processes N_n statistically independent over n. The observations u_n are encoded and transmitted by independently operating encoders indexed by $n = 1,2,...,N$. The source processes are Gaussian distributed $\mathcal{N}(\mu_0, \sigma_0^2)$ with mean $\mu_0 = 0$ and variance $\sigma_0^2 = 1$. The noise processes are also Gaussian distributed $\mathcal{N}(\eta_n, \lambda_n^2)$ with mean $\eta_n = 0$ and variance $\lambda_n^2 = \lambda$, $n = 1,2,\ldots,N$. We define the SNR in the observation as

$$\mathrm{SNR_O} = 10 \cdot \log_{10}\left(\frac{\sigma_0^2}{\lambda^2}\right) \text{ in dB}.$$

For each encoder n: We assume that the continuous-valued source symbols u_n are transduced onto discrete-valued indices i_n via a scalar quantization stage. We consider the symmetric case where the quantizer resolution is constant over all encoders and choose, depending on the considered setup, a resolution of $L = 32, 64$ and 128 indices for quantization, corresponding to a *source rate* of



Simulation results for the symmetric CEO problem with $N = 3$ encoders. The performance for source rates $R_s = 5, 6$ and 7 bit per index and constant data rate $R = 5$ bit per codeword is compared to the theoretical R/D bound.

$R_s = 5, 6$ and 7 bit per index. The cyclic index assignments of K_n codewords are chosen such that a constant *data rate* of $R = 5$ bit per codeword for all quantizer setups and all encoders is achieved.

The optimality criterion of interest is the mean squared error and we use a decoding function d based on conditional mean estimation as presented in [5].

To evaluate the performance of our coding strategies, we measure the Output SNR for U_0, as given by

$$\text{Output SNR} = 10 \cdot \log_{10}\left(\frac{u_0^2}{(u_0 - \hat{u}_0)^2}\right) \text{ in dB},$$

versus the $\mathrm{SNR_O}$.

Figure 3 illustrates the performance of the system for $N = 3$ sources without compression by cyclic index assignments (i.e. when choosing $R_s = 5$ bit per index) and the performance obtained when index assignments are employed (i.e. when choosing $R_s = 6$ and 7 bit per index), in comparison to the theoretical limit given by the sum rate-distortion function (R/D) computed according to [4].

The numerical results were obtained by simulations implemented in Matlab R14. The curves show the performance of the whole system after simulating 100000 realizations of U_0 and the vertical bars show the 95% confidence interval.

The numerical results show that, over a wide range of correlation values, our low-complexity, Diophantine index assignment techniques lead to significant performance gains over standard scalar quantization and come close to the theoretical optimum for the considered scenario.

Bibliography

[1] T. J. Flynn and R. M. Gray, "Encoding of correlated observations," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 6, pp. 773–787, 1987.

[2] G. Maierbacher and J. Barros, "Low-complexity coding and source-optimized clustering for large-scale sensor networks." accepted for publication in the ACM Transactions on Sensor Networks. To appear in Vol. 5, Iss. 3, Aug. 2009. Available from `http://arxiv.org/abs/0809.1330`.

[3] ——, "Diophantine index assignments for distributed source coding," in *Proceedings of the 2007 IEEE Information Theory Workshop (ITW 2007) - Frontiers in Coding*, Lake Tahoe, California, USA, 2007.

[4] J. Chen, X. Zhang, T. Berger, and S. B. Wicker, "An upper bound on the sum-rate distortion function and its corresponding rate allocation schemes for the CEO problem," *Special Issue of JSAC, On Fundamental Performance of Wireless Sensor Networks*, May 2004.

[5] G. Maierbacher and J. Barros, "Low-complexity coding for the CEO problem with many encoders," in *Twenty-sixt Sypposium on Information Theory in the Benelux*, Brussels, Belgium, 2005.

Source-Optimized Clustering and Distributed Source Coding

Gerhard Maierbacher and João Barros

Motivated by the design of low-complexity distributed quantizers and iterative decoding algorithms that leverage the correlation in the data picked up by a large-scale sensor network, we address the problem of finding correlation preserving clusters. We develop a hierarchical clustering algorithm that minimizes the Kullback Leibler Distance between known and approximated source statistics and show how the clustering result can be exploited in the design of distributed quantizers and source-channel decoder implementations of manageable complexity.

Introduction

In distributed sensing scenarios, where correlated data has to be gathered by a large number of low-complexity, power-restricted sensors, efficient source coding and data gathering techniques are key towards reducing the required number of transmissions and enabling extended network life-time.

Inspired by the seminal work of Slepian and Wolf, characterizing the fundamental limits of separate encoding of correlated sources, several authors have contributed with coding solutions. Focusing on scalar quantization, proposes to eliminate the redundancy in the source observations by index-reuse, considering the overall end-to-end distortion as optimization criteria.

Clustering algorithms, largely inspired by contributions in statistical data analysis, have proved to be useful in the context of sensor networks, particularly in the design of energy-efficient and decentralized protocols.

The main goal of this work is to ensure the *scalability* of distributed quantization, i.e. its applicability to scenarios with a very large number of encoders (100 or more), for which *source*-optimized clustering provides a natural solution. Previous work [1] along this line presented a solution for the scalability problem on the decoding side by running the sum-product algorithm on a carefully chosen factor graph approximation of the source correlation. Focusing on the encoding side, we now provide a scalable solution for distributed quantization based on source-optimized hierarchical clustering. The main idea is to exploit correlation preserving clusters for, both, the design of distributed quantizers and an efficient decoder implementation. We present numerical results to underline the efficiency and the scalability of the proposed approach.

Clustering Algorithm and Factor Graph Approximation

The main idea of our approach is to find clusters of sensors, i.e. to find subsets of sensors, in which strong correlations between the sensor measurements exist and, then, to use standard distributed source codes, e.g. distortion optimized index assignments, for the sensors within those clusters. Adopting this clustering approach, we are provided with an inherently scalable encoding solution, feasible for a large number of sensors. In order to find suitable clusters, we propose a method based on hierarchical clustering, using the Kullback-Leibler Distance between the given source statistics and a given factor graph approximation as optimization criteria.

Since this factor graph is also used at the decoder, the correlations within the clusters can be exploited to improve the decoding result.

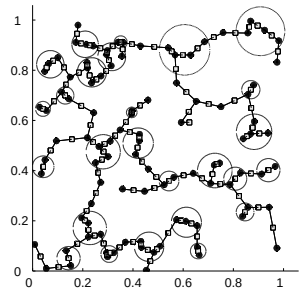
Details about the hierarchical clustering algorithm itself as well as the linking procedure that is required to construct the factor graph can be found in [2] and [3].

Figure 1 shows the obtained clusters and the resulting factor graph for an exemplary scenario of $M = 100$ uniformly distributed sensors.

Results and Discussion

To underline the effectiveness and efficiency of our low-complexity coding strategies, we present numerical performance results for an exemplary scenario with $M = 100$ uniformly distributed sensors.

The measurements u_m at each sensor $m = 1,2,\ldots,M$ are Gaussian distributed $\mathcal{N}(0,1)$. The vector of all sensor measurements $\mathbf{u} = (u_1,u_2,\ldots,u_M)^T$ is distributed according to a multivariate Gaussian distribution $\mathcal{N}(\mathbf{0}_M,\mathbf{R})$, where the correlation between a pair of sensors u_k and u_l decreases exponentially with the distance $d_{k,l}$ between them, such that $\rho_{k,l} = \exp(-\beta \cdot d_{k,l})$. Since



Exemplary scenario with $M = 100$ uniformly distributed sensors. The depicted factor graph was constructed by finding KLD optimized clusters with a maximum size of four sources per cluster, as indicated by circles, linked together by choosing one source within each cluster to establish the link between the clusters.

the performance of our techniques depend on the correlations between the sensors, we consider two different source models, one with $\beta = 0.5$ (strongly correlated sensor measurements) and one with $\beta = 2$ (weakly correlated measurements).

The encoders at each sensor $m = 1, 2, \ldots, M$ consist of a standard scalar quantization stage followed by distortion optimized index assignments based on index-reuse. The quantizer resolution of L levels and the transmission rate of Q bit are chosen to be constant over all encoders $m = 1, 2, \ldots, M$.

The clusters are derived based on the proposed clustering algorithm with a maximum cluster size of four sources per cluster, see [2] and [3] for details.

The factor graph used for decoding is then constructed based on the clusters, which are linked together by choosing one source within each cluster to establish the link between the clusters, see [2] and [3] for details. Figure 1 shows the factor graph obtained for the considered scenario with $\beta = 0.5$.

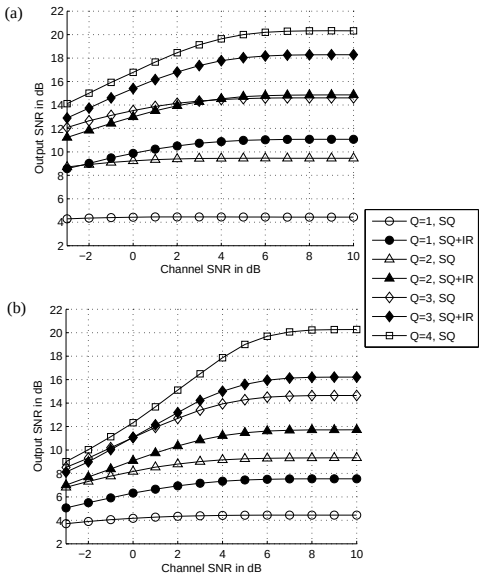
Using the derived factor graph, the decoder is based on the sum-product algorithm as described in [2] and [3].

To evaluate the performance, we measure the output signal-to-noise ratio (SNR) given by

$$\text{Output SNR} = 10 \cdot \log_{10} \left(\frac{||\mathbf{u}||^2}{||\mathbf{u} - \hat{\mathbf{u}}||^2} \right) \text{in dB} \qquad (1)$$

versus the channel SNR $= 10 \cdot (E_s/N_0)$ in dB averaged over a $M \times 10000$ source samples.

The simulation results of our system are depicted in Figure 2 (a) for strongly and in Figure 2 (b) for weakly correlated sources. In both scenarios, we consider the performance achieved when using scalar quantization alone at the encoder, i.e. where the performance is mainly governed by the properties of the decoder, and the performance achieved when scalar quantization with a subsequent index-reuse is used for encoding.



Simulation results. Performance of the system with $M = 100$ sensors for correlation factor $\beta = \{0.5,\ 2\}$ when simple scalar quantization (SQ) alone and scalar quantization with a subsequent index-reuse (SQ+IR) is used at the encoder. All encoders use identical transmission rates of Q bit per sample.

Our simulation results reveal, that despite the simplicity of the proposed encoding techniques, significant performance gains can be achieved by the proposed joint encoding/ decoding approach.

Possible extensions of the presented work include other classes of index assignments, e.g. based on channel codes with appropriate distance properties.

Bibliography

[1] J. Barros and M. Tuchler, "Scalable decoding on factor trees: a practical solution for wireless sensor networks," *IEEE Transactions on Communications*, vol. 54, no. 2, pp. 284–294, Feb. 2006.

[2] G. Maierbacher and J. Barros, "Source-optimized clustering for distributed source coding," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'06)*, San Francisco, CA, USA, 2006.

[3] ——, "Low-complexity coding and source-optimized clustering for large-scale sensor networks." accepted for publication in the ACM Transactions on Sensor Networks. To appear in Vol. 5, Iss. 3, Aug. 2009. Available from `http://arxiv.org/abs/0809.1330`.

Wireless Information-Theoretic Security

João Barros, Miguel Rodrigues and Tiago Vinhoza

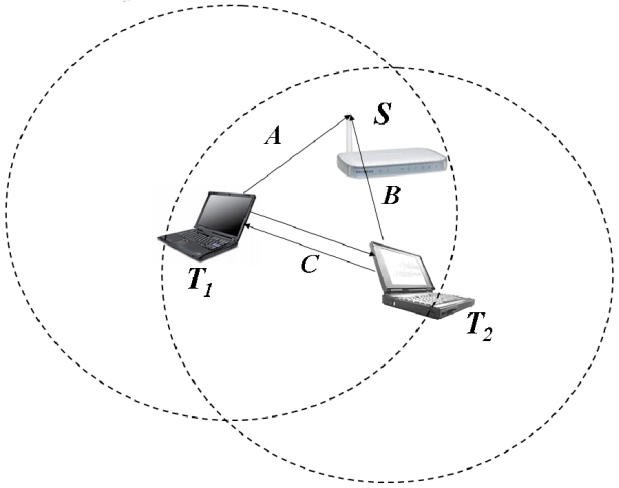
Contemporary secured communication systems adopt a modular approach in which data processing, transmission and encryption are carried out separately. The typical purpose of the physical layer is to guarantee error-free transmission, usually through the use of error control coding, whereas encryption is performed at a higher layer in the protocol stack, where the issue of errors in the data can be ignored. State-of-the-art encryption algorithms are thus insensitive to the characteristics of the communications channel, relying on mathematical operations assumed to be hard to compute, such as prime factorization and the discrete logarithm function. However, this modular approach for data security becomes increasingly difficult to justify if we consider that: (a) the underlying intractability assumptions may be wrong, (b) efficient attacks could be developed, (c) the advent of quantum computers is likely to compromise this type of encryption, and (d) fast and reliable communications over ad hoc wireless networks require light and effective security architectures.

As an alternative, information-theoretic results show the benefits of exploiting the randomness of the communication channels at the physical layer in the network to guarantee that the sent messages cannot be decoded by a third party, maliciously eavesdropping on the wireless medium: security is ensured not relatively to a hard mathematical problem but by the physical uncertainty inherent to the noisy channel - the crux of Shannon's information theory. Building on Shannon's notion of perfect secrecy [1], seminal works by Wyner [2] and by Csiszár and Körner [3] prove that there exist channel codes guaranteeing both robustness to transmission errors and a prescribed degree of data confidentiality. The secrecy capacity of the Gaussian wiretap channel, i.e. the maximum transmission rate at which an eavesdropper is unable to decode any information, was characterized by Leung and Hellman [4].

More recently, information-theoretic security witnessed a renaissance arguably due to the work of Maurer [5], who proved that even when the legitimate users have a worse channel than the eavesdropper, it is possible for them to generate a secret key through public communication over an insecure yet authenticated channel.

Work Done so far

Motivated by the general problem of securing transmissions over wireless channels, we considered the impact of fading on the secrecy capacity. Our contributions were the following [6]: (a) an information-theoretic formulation of the problem of secure communication over wireless channels; (b) a characterization of the secrecy capacity of single-antenna quasi-static Rayleigh fading channels in terms of outage probability; (c) a simple analysis of the impact of user location on the achievable level of secrecy; (d) a rigorous comparison with the Gaussian wiretap channel evidencing the benefits of fading towards achieving a higher level of security. Among the different conclusions to be drawn from our results perhaps the most striking one is that, in the presence of fading, information-theoretic security is achievable even when the eavesdropper's channel has a better average signal-to-noise ratio than the main channel.



Example of a wireless network with potential eavesdropping. Terminals T_1 e T_2 communicate with a base station S over a wireless medium (channels A and B). By listening to the transmissions of terminal T_1 (through channel C), terminal T_2 may acquire confidential information. If T_1 wants to change a secret key or guarantee the confidentiality of its transmitted data, it can exploit the *physical* properties of the wireless channel to secure the information by *coding* against terminal T_2.

For secrecy purposes, fading turns out to be a friend and not a foe.

In principle, secure communications over wireless quasi-static fading channels can be achieved with codes designed for the Gaussian wiretap channel; however, although the secrecy capacity of the Gaussian wiretap channel has been fully characterized, the design of practical coding schemes is still an open problem. In contrast, previous results on secret key agreement by public discussion and privacy amplification support the idea that the generation of information-theoretically secure keys from common randomness is a somewhat less difficult problem.

Based on the aforementioned results, we developed a practical secure communication protocol [7], which uses a four-step procedure to ensure wireless information-theoretic security: (a) common randomness via opportunistic transmission, (b) message reconciliation, (c) common key generation via privacy amplification, and (d) message protection with a secret key. A reconciliation procedure based on multilevel coding and optimized low-density parity-check (LDPC) codes was introduced, which allows to achieve communication rates close to the fundamental security limits in several relevant instances. Finally, a set of metrics for assessing average secure key generation rates was established, and it was shown that the protocol is effective in secure key renewal–even in the presence of imperfect channel state information.

Security is ensured not relatively to a hard mathematical problem but by the physical uncertainty inherent to the noisy channel - the crux of Shannon's information theory.

Future Work

Using the mathematical tools of information theory we will try to characterize the achievable transmission rates subject to a confidentiality criterion, i.e., the secrecy capacity of several fundamental classes of multiple-user channels, such as the multiple access channel (many-to-one), broadcast channel (one-to-many), interference channel (cognitive radio with side information on the sent messages), relay channel (with user cooperation) and networks of relay channels (multi-hop communication). These channels can be viewed as the building blocks of larger and more complex communication networks, which can be described by graphs and analyzed in terms of maximum throughput with security constraints. The key challenge in these setups with multiple senders is the impact of interference between their signals when transmitted over the common channel.

Building on the results for discrete memoryless channel models, we will proceed to more sophisticated wireless channel models that, by taking into account phenomena such as attenuation and multi-path, come closer to the physical reality of the wireless medium.

Cooperation

Part of this research was done in cooperation with Prof. Steven W. McLaughlin, from Georgia Institute of Technology and Matthieu Bloch, from University of Notre Dame.

Bibliography

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. Journ.*, vol. 29, pp. 656–715, 1949

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. Journ.*, vol. 54, pp. 1355–1387, 1975.

[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] S. K. Leung, M. E. Hellman, "The gaussian wiretap channel". *IEEE Trans. Inf. Theory*, vol. 24, no.4, pp. 451-456, July 1978.

[5] U. Maurer, "Secret key agreement by public discussion from common information". *IEEE Trans. Inf. Theory*, vol. 39, no.3, pp. 733-742, May 1993.

[6] J. Barros, M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels". *Proc. International Symposium on Information Theory*, pp. 356-360, July 2006.

[7] M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin, "Wireless Information-Theoretic Security". *IEEE Trans. Inf. Theory*, June 2008.

instituto de telecomunicações

Secure Quantization

João Almeida, Gerhard Maierbacher and João Barros

We propose a low-complexity encoding mechanism based on secure quantization [1]. The key idea is to make use of randomized index assignments to induce confusion on the eavesdropper. Privacy can be measured in terms of end-to-end distortion, where the objective is to maximize the distortion at the eavesdropping receiver and minimize the distortion between legitimate terminals.

Introduction

Classical scalar quantization has so far been oblivious to standard security considerations. The general course of action when ensuring secrecy in digital communications is to use cryptographic primitives, which are most often independent of the employed source coding mechanisms. To use this modular approach guarantees both reliable and secure information transmission. However, when applied to applications involving large volumes of data and strict delay constraints, the complexity of encryption and decryption processes often results in an undesirable loss of computational efficiency. Encouraged by recent results in information-theoretic security, we turn our attention to the design of lighter security mechanisms based on information-theoretical principles. Seeking a scheme under which secure communications could be evaluated, Wyner proposed *wiretap channel* model [2]. The model assumes that an eavesdropper observes a degraded version of the information sent to a legitimate receiver through the *main channel*. Under the *wiretap channel* model, Wyner proved the existence of channel codes capable of guaranteeing both reliable and secure data transmission. Secrecy levels were measured in terms of of secrecy capacity.

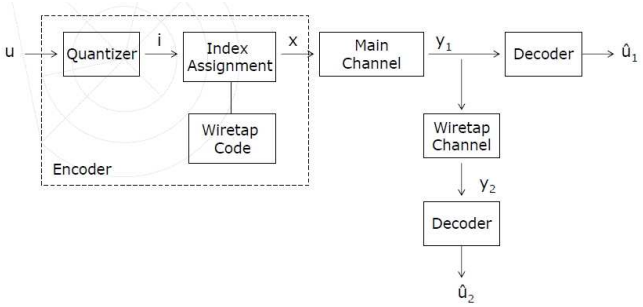
Although its existence is proven, practical construction of coding schemes capable of reaching the secrecy capacity is an open problem for most cases of interest.

Secure Quantization

Under a different perspective, we seek to explore the trade-off between privacy and communication with high fidelity. We assume continuous-valued sources and measure the privacy level of our communication system by computing the minimum achievable distortion at the eavesdropping receiver. We focus on the design of scalar quantizers with a twofold objective (a) achieve low distortion at the legitimate receiver and (b) maximize the distortion at the eavesdropper.

Intrigued by the non-obvious balance between reliability and security, we consider the problem of optimizing the index assignment stage of quantization for a wiretap scenario in which the distance between the distortions of the legitimate receiver and the eavesdropper is the main figure of merit. Our main contributions are as follows:

- *Coding Concept*: assuming a degraded wiretap channel, we combine a scalar quantizer with not one but multiple index assignments, one of which is chosen randomly at each transmission;
- *Design Algorithm*: we develop an algorithm for optimizing the index assignment stage under the aforementioned conditions;



Communication system setup.

Coding Concept

In contrast to a classical encoder design, in which the quantization step is followed by an unique index assignment, our randomized approach seeks to deceive the eavesdropper by picking one of multiple index assignments at random for each quantized symbol. The set of index assignments can be viewed as a *wiretap code*. Due to the stochastic nature of the encoder, it is necessary for the decoder to be informed about the chosen index assignment for each quantizer output. Hence, the encoder output is a block of binary data composed by the representation of the selected index assignment and the corresponding channel codeword.

▪ Messages

x1	x2	x3	x4	x5
	B_m		B_q	

▪ Wiretap Code

i	C0	C1	C2	C3
0	011	110	101	011
1	100	001	000	100
2	111	101	110	111
3	001	011	010	000
4	010	111	111	010
5	110	100	011	001
6	000	000	001	101
7	101	010	100	110

Example of encoder output and wiretap code.

Upon data transmission over the main channel, the legitimate receiver obtains a vector of channel output symbols. At the same time, an eavesdropper has access to a noisy version of the output of the main channel. Both receivers observe the the channel symbols corresponding to the the selected index assignment. After recognizing the encoding index assignment, they form source estimates with the subsequent channel symbols and decode accordingly. We consider the case where both the main channel and the wiretap channel are modeled by binary symmetric channels.

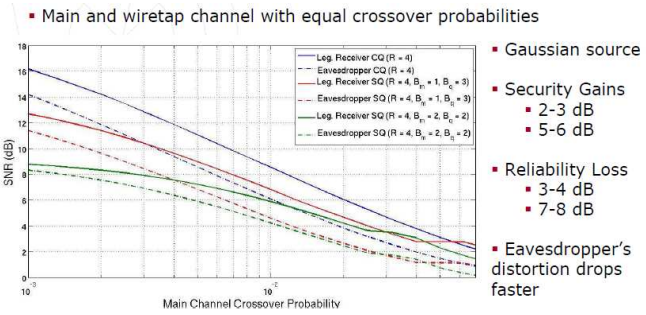
The main idea behind the secure quantizer is to use the allocated bits for index assignments to increase uncertainty of the eavesdropper. Since he observes the outputs of a channel prone to transmission errors, his decoder is more likely to end up with the wrong index assignment, which in turn leads to higher end-to-end distortion. Although in a smaller scale, we can also expect to see higher distortions at the legitimate receiver, due to possible transmission errors of the main channel. Clearly, we witness a trade-off between end-to-end distortion and privacy levels. The loss of fidelity may be bearable if in return we are able to severely impair the eavesdropper from acquiring information about the transmitted symbols.

Index Assignment Optimization

Clearly, the wiretap code choice affects end-to-end distortion, so it is essential to determine adequate index assignments that achieve desirable distortion values. Due to the prohibitive complexity of an optimum search, we consider the construction of sub-optimal index assignments by means of feasible search algorithms that target an acceptable trade-off between fidelity and privacy. For this purpose, we propose an iterative procedure which is based on a greedy approach. The corner stone of the algorithm is an elementary index assignment modification step, aiming at maximizing the distortion difference between both receivers. This step is repeated until index assignment sets with arbitrarily close distortion difference are found.

Conclusion

Intrigued by the design of practical secure coding schemes, we proposed a secure scalar quantizer using multiple index assignments. An index assignment optimization algorithm was developed. The algorithm searches for index assignments satisfying both minimum and maximum distortion criteria for the legitimate receiver and the eavesdropper, respectively. For the Gaussian source, the obtained results demonstrate that the eavesdropper's end-to-end distortion drops relatively fast in contrast to a classical quantizer design albeit at some cost in terms of added distortion at the legitimate receiver.



Simulation results comparing performance of classical quantizer (CQ) and secure quantizer (SQ).

Bibliography

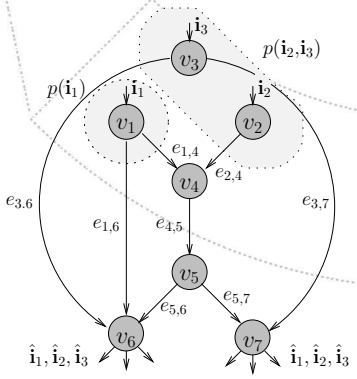
[1] J. Almeida, G. Maierbacher, and J. Barros, "Low-complexity index assignments for secure quantization," in *Proc. 43rd Annual Conference on Information Sciences and Systems (CISS'09)*.

[2] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. Journ.*, vol. 54, pp. 1355–1387, 1975.

A First Step Towards Practical Joint Source-Network Coding

Gerhard Maierbacher and João Barros

Network coding has proven to be a key enabler towards achieving the throughput in networks with possibly more than one data source and several sinks as e.g. shown in Figure 1. The key idea is to replace routing operations that have to be performed at intermediate network nodes by coding operations. Those coding operations have the advantage that (opposed to routing) packets can be combined as they traverse the network, which allows for more flexibility, while distributing the data throughout the network. A sink node uses the received packets and deduces from their content (which generally represents a combination of several packets from different sources) the data originally intended for that sink.



Exemplary network with three source nodes v_1, v_2, v_3 and two sinks v_6, v_7. In this particular scenario, the source symbols $\mathbf{i}_1$ are independent of the source symbols $\mathbf{i}_2$ and $\mathbf{i}_3$, as indicated by the shaded areas. As discussed in [1], joint decoding is required here.

Considering the case of correlated sources, where data from one source already contains some information about other sources, information theoretic results tell us that the amount of data, which needs to be transmitted from the source to the sink (at a given quality), can be reduced by considering the source correlations within the coding scheme. Distributed source coding techniques allow us to do so.

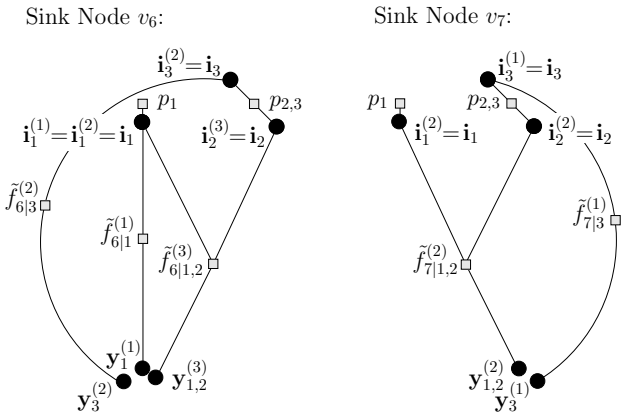
In scenarios where correlated source data needs to be communicated over a network it is possible to perform distributed source coding and network coding separately. However, this approach is shown to be non-optimal for certain scenarios. The solution to this problem would be to perform *joint* source-network coding which is a highly challenging task mostly due to the complexity of the decoder. The problem lies within the fact that the decoding complexity of distributed source coding schemes generally increases exponentially with the number of source nodes.

We show how to perform near-optimal, yet computationally tractable, joint source-network decoding and provide a proof-of-concept in form of a working implementation.

Statistical Models and Iterative Decoding

The largest challenge in providing a joint source-network coding solution for large-scale networks is to overcome the complexity problem at the decoder. The high decoding complexity results from the fact that, in general, the (joint) source source statistics have to be considered within the decoding operation to obtain an optimal result. The same problem also appears e.g. when performing distributed source coding alone, i.e. when no additional network coding is considered. In previous work on scalable coding solutions for sensor networks [2], we provided a near-optimal, yet computationally tractable, solution to this problem. The core of the solution was to construct a (graphical) model, representing the (joint) source statistics, which can be used for an efficient decoder implementation. Considering the case of joint source-network coding, the same techniques can be employed here. After finding a statistical representation of the network itself (i.e. for the packets traversing the network), we are able to use this representation together with the source model to obtain a joint source-network decoding model. This model can then be exploited for an efficient decoder implementation. Details are neglected here, but Figure 2 provides some intuition on how the decoding model describes the statistical dependencies within system.

Since it is possible to consider the derived decoding model as a *factor-graph*, we are able to employ the iterative *sum-product algorithm*, which allows us to split the complex, global decoding operation into (exponentially) less complex, local operations. This gives rise to an efficient implementation and it is actually possible to show that in many practical scenarios the complexity of the proposed scheme only increases linearly with the number of nodes.



Decoding model for the sinks v_6 and v_7 in the scenario presented before. The graphical model represents the statistical dependencies within the system. The black, round nodes represent the random variables within the system and the gray, square nodes represent the statistical dependencies between the connected variables.

Proof-of-Concept and Conclusion

In order to provide a proof-of-concept, we implemented the decoders for the scenario depicted in Figure 1 using the decoding models depicted in Figure 2.

The (discrete-valued) source symbols $\mathbf{i}_s$, $s = 1,2,3$, are considered to be the quantized versions of continuous-valued source samples $\mathbf{u}_s$, which are jointly distributed according to a multivariate Gaussian distribution, emulating the scenario in [1]. In this model the source symbols $\mathbf{u}_2$ and $\mathbf{u}_3$ are correlated with a correlation coefficients ρ ranging from 1 (i.e. fully correlated) to 0 (i.e. independent).

The transmission rates are chosen adequately as described in [1], where in some cases we also allow for a greater rate of δ bits in order to improve the decoding results.

In our experiments we use 10^6 samples for each source and each simulation. We quantify the decoding performance at sink node v_t, decoding the discrete-valued source symbols $\mathbf{i}_s$ to form the reconstruction values $\hat{\mathbf{i}}_{s,t}$, in terms of the error probability $P_{s,t}$ and, similarly, we consider the output signal-to-noise ratio $\mathrm{SNR}_{s,t} = -10\log_{10} E\{(\mathbf{u}_s - \hat{\mathbf{u}}_{s,t})^2\}$ in dB to evaluate the performance in the case of continuous-valued sources.

Numerical results for the presented setup and several values of δ are summarized in the Table.In Case (a) where $\mathbf{u}_2$ and $\mathbf{u}_3$ are fully correlated (i.e. $\mathbf{u}_2 = \mathbf{u}_3$) and Case (d) where $\mathbf{u}_2$ and $\mathbf{u}_3$ are statistically independent, we obtain optimal results with a error probability $P_{s,t} = 0$ and an output $\mathrm{SNR}_{s,t} = 14.6$ dB. The optimality of the results is expected, since in each of those cases the system degrades and can be represented by an equivalent system that does not require source correlations for decoding. For Case (b) and (c) we need the correlations for decoding. We observe that

ρ	1	0.988		
δ [bit]	0	0	0.585	1
$P_{1,6}=P_{2,6}$	0	0	0	0
$P_{3,6}$	0	82.6e-3	43e-6	18e-6
$P_{1,7}=P_{2,7}$	0	65.8e-3	43e-6	11e-6
$P_{3,7}$	0	0	0	0
$\mathrm{SNR}_{1,6}$ [dB]	14.6	14.6	14.6	14.6
$\mathrm{SNR}_{2,6}$ [dB]	14.6	14.6	14.6	14.6
$\mathrm{SNR}_{3,6}$ [dB]	14.6	12.6	14.6	14.6
$\mathrm{SNR}_{1,7}$ [dB]	14.6	8.29	14.6	14.6
$\mathrm{SNR}_{2,7}$ [dB]	14.6	12.8	14.6	14.6
$\mathrm{SNR}_{3,7}$ [dB]	14.6	14.6	14.6	14.6
Case	(a)	(b)	(b1)	(b2)

ρ	0.881			0
δ [bit]	0	0.322	0.585	0
$P_{1,6}=P_{2,6}$	0	0	0	0
$P_{3,6}$	28.2e-3	5.20e-3	430e-6	0
$P_{1,7}=P_{2,7}$	23.7e-3	4.50e-3	468e-6	0
$P_{3,7}$	0	0	0	0
$\mathrm{SNR}_{1,6}$ [dB]	14.6	14.6	14.6	14.6
$\mathrm{SNR}_{2,6}$ [dB]	14.6	14.6	14.6	14.6
$\mathrm{SNR}_{3,6}$ [dB]	9.40	12.3	14.2	14.6
$\mathrm{SNR}_{1,7}$ [dB]	9.17	13.0	14.5	14.6
$\mathrm{SNR}_{2,7}$ [dB]	9.87	12.5	14.2	14.6
$\mathrm{SNR}_{3,7}$ [dB]	14.6	14.6	14.6	14.6
Case	(c)	(c1)	(c2)	(d)

already for $\delta = 0$ we obtain reasonably good performance by our joint source-network decoding approach. Furthermore, considering Case (b1), (b2), (c1) and (c2), we observe that if we are willing to increase the transmission rate by a small amount $\delta > 0$ then the overall performance improves rapidly, which underlines the capabilities of the decoder to effectively exploit additional redundancy (in the received packets) to improve the overall decoding result.

Bibliography

[1] A. Ramamoorthy, K. Jain, P. A. Chou, and M. Effros, "Separating distributed source coding from network coding," *IEEE/ACM Trans. Netw.*, vol. 14, no. SI, pp. 2785–2795, 2006.

[2] G. Maierbacher and J. Barros, "Low-complexity coding and source-optimized clustering for large-scale sensor networks." accepted for publication in the ACM Transactions on Sensor Networks. To appear in Vol. 5, Iss. 3, Aug. 2009. Available from `http://arxiv.org/abs/0809.1330`.

Flooding in Random Networks

Sérgio Crisóstomo and João Barros

Information dissemination in communication networks is a key function whose effectiveness depends both on the chosen dissemination algorithm and on the underlying network topology. We study information dissemination in networks modeled by different kinds of random graphs. Algorithms under investigation are probabilistic flooding, multipoint relaying, and network-coded flooding.

Introduction

Typically, information dissemination algorithms resort to replication based forwarding where nodes replicate and forward the information they receive, preserving message's integrity. The spectra of information dissemination algorithms was recently enlarged by the advent of the network coding (NC) paradigm where the message integrity principle is abandoned. This paradigm is based on the simple but important observation that the act of combining different information flows in intermediate nodes can lead to faster and more robust dissemination of information.

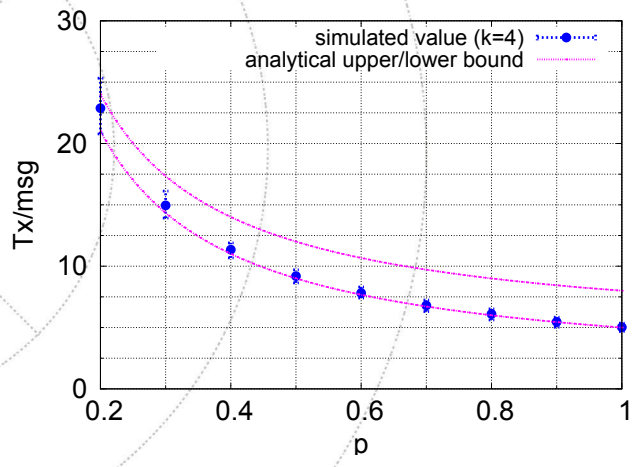
Dissemination algorithms can be further categorized in two main classes: In the probabilistic class messages are conveyed according to a set of probabilistic rules, whereas the deterministic class advocates deterministic algorithms.

Our work addresses the following aspects:

- Analysis of how dissemination algorithms need to be tuned to ensure global information outreach;
- Analysis of how the topology of the underlying network influences the performance of the information dissemination;
- Comparison between competing information dissemination paradigms and algorithms;
- Design of new efficient dissemination algorithms.

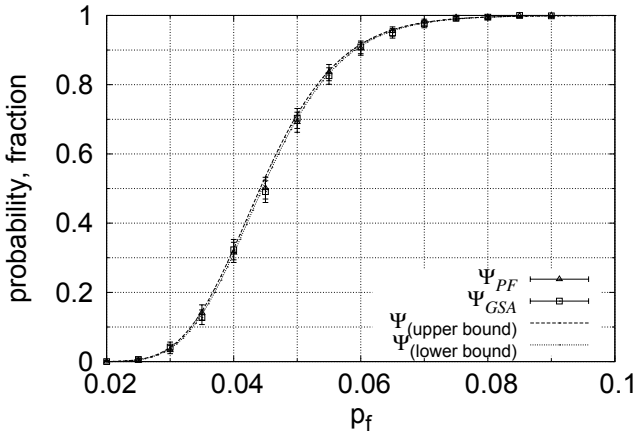
Research Results

In the last year, our research led to the publication or acceptance for publication of three papers in international conferences. In the first one (ICCSC 2008, Shanghai, China, May 2008, [1]), we address the following questions: (a) How does NC based flooding competes against replication based flooding? (b) What benefits may we expect from the use of NC based flooding? (c) How does the topology influences the behavior of NC based flooding? To answer these questions we performed an analytical and simulation study where we characterized the benefits of NC based flooding in terms of number of transmissions per source message and in terms of delay (see Fig. 1). Our work shows that in networks modeled by Erdős Rényi random graphs and Random Geometric graphs, the number of transmissions required to flood a message with the NC flooding algorithm under consideration is asymptotically independent of the number of nodes. The simulation results comparing NC flooding with Multipoint Relaying based flooding corroborate the benefits in terms of number of transmissions and delay that we obtain by the use of network coding.



Number of Transmissions per Message using Network Coded Flooding in Erdős Rényi Random Graphs as function of the edge probability p, for a number of nodes $n = 50$. Comparison of the simulated results with the analytical upper and lower bounds.

In another paper (ICCS 2008, Guangzhou, China, November 2008, [2]) we address information dissemination in broadcast environments with Small-world network (SWN) topologies. We investigated how the topological properties of SWNs (in particular small network diameters and large clustering coefficients) enhance the spread of information under distinct information dis-



Global outreach probability Ψ for probabilistic flooding in Erdős Rényi random graphs as function of the message forwarding probability p_f. The number of nodes is $n = 1000$ and the edge probability $p_e = 0.15$. Comparison of the simulated real probabilistic flooding (PF), the simulated graph sampling (GS) approach, and lower and upper analytical bounds. Each simulated data point (with its respective 95% confidence interval limits) is obtained from 1000 random graphs, where a flooding is performed on each graph.

semination paradigms (i.e. network coded and replication based paradigms). We show, both analytically and through simulation, that network coding requires a smaller number of transmissions and shorter propagation delays, conjugated with impressive steadiness under distinct topological configurations.

Finally, in a paper accepted for publication (ICC 2009, Dresden, Germany, June 2009, [3]) we address the problem of which forwarding probability must be used to ensure global information outreach with probabilistic information dissemination algorithms. We first address probabilistic flooding algorithms operating over networks modeled as Erdős Rényi random graphs. We derived tight bounds for the probability of global outreach as function of the forwarding probability and we complemented the analytical results with numerical simulations (see Fig. 2).

Acknowledgements

Joint work with Christian Bettstetter and Udo Schilcher from the University of Klagenfurt, Austria.

Bibliography

[1] S. Crisóstomo, J. Barros, and C. Bettstetter, "Flooding the Network: Multipoint Relays versus Network Coding," in *Proc. of the IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008)*, Shanghai, China, May 2008.

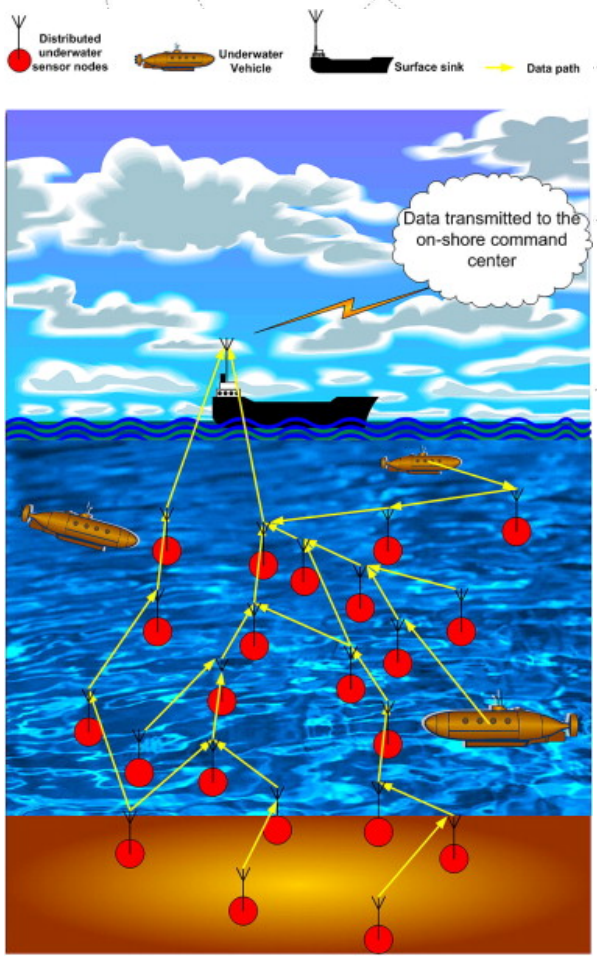
[2] S. Crisóstomo, , J. Barros, and C. Bettstetter, "Network Coding with Shortcuts," in *Proc. of IEEE International Conference on Communication Systems (ICCS 2008)*, Guangzhou, China, November 2008.

[3] S. Crisóstomo, U. Schilcher, J. Barros, and C. Bettstetter, "Analysis of Probabilistic Flooding: How do we Choose the Right Coin?" in *Proc. of IEEE International Conference on Communication (ICC 2009)*, Dresden, Germany, June 2009.

Energy-Efficient Routing in Underwater Sensor Networks

Rui Prior

Underwater wireless sensor networks consist of a certain number of sensors and vehicles that interact to collect data and perform collaborative tasks. Designing energy-efficient routing protocols for this type of network is essential and challenging because sensor nodes are powered by batteries, which are difficult to replace or recharge, and because underwater communications are severely affected by network dynamics, large propagation delays and high error probability of acoustic channels.



Underwater Wireless Sensor Networks (UWSNs)

Introduction

The sea is a fascinating large expanse of water that has always attracted people who wanted to solve its mysteries. For centuries the access of human beings to the sea was limited to the surface or the nearby water, because the researchers had to use wire-line instruments and sampling equipment located at the sea surface. This fact restricted the scientific research operations.

Nowadays there is a growing need of underwater monitoring (e.g., for exploration of natural undersea resources, gathering of scientific data or detection of marine incidents such as chemical pollution or oil spill) but the existing technologies do not measure up to the demanding requirements. Small-scale underwater acoustic networks (UANs) are associations of nodes that collect data using remote telemetry or assuming point-to-point communication. Remote telemetry with high precision is very expensive. With point-to-point communication, a multi-access technique is not used because the nodes are sparsely deployed. Besides, UANs are usually fixed, either anchored in the sea floor or attached to buoys or GPS systems. Consequently, a new concept of low-cost more easily deployable underwater networks with less restricted conditions has emerged: underwater wireless sensor networks (UWSNs). This kind of networks must be scalable, mobile and capable of self-organization (by exchanging configuration, location and movement information). They eliminate the need for cables and do not interfere with shipping activity.

Characteristics of UWSNs

RF radio does not work well in the underwater environment because radio waves propagate only at extra low frequencies (30–300 Hz) and require large antennae and high transmitter powers; optical waves are severely affected by scattering, and, as a result, underwater networks are based on the propagation of acoustic waves.

UWSNs are very different from ground-based existing networks due to the intrinsic properties of the underwater environments. The networks suffer from:

- Large propagation delays:
  The propagation speed of acoustic signals in water is about

1.5×10^3 m/s, five orders of magnitude lower than the radio propagation speed (3×10^8 m/s); the resulting large propagation delays seriously impair localization and time synchronization.

- Node mobility:
  Underwater sensor networks move with water current (empirical observations suggest that water current moves at a speed of 3–6 km/h in a typical underwater condition.
- High error probability of acoustic underwater channels:
  The underwater acoustic communication channel has a limited bandwidth capacity (of the order of KHz) that depends on transmission range and frequency, has variable delays and suffers high bit error rates, which are caused by noise, multi-path and Doppler spread. Consequently, temporary losses of connectivity can be experienced (shadow zones).

The stringent network operation conditions pose a motivation for doing research at each layer of the protocol stack.

Energy concerns in UWSNs

Energy saving is a major concern in UWSNs because sensor nodes are powered by batteries and it could be difficult to replace or recharge batteries in aquatic environments. In acoustic networks the power required for transmitting is typically about 100 times more than the power required for receiving.

> The design of robust, scalable and energy-efficient routing protocols in this type of networks is an important research issue.

Most existing data forwarding protocols proposed for ground-based sensor networks cannot be directly applied because they have been designed for stationary networks. The existing multi-hop ad hoc routing protocols are not adequate because they employ flooding techniques for packet routing (at least during the route discovery mechanism) that would lead an UWSN easily to energy exhaustion because in UWSNs the medium is highly variable and the routing overhead due to updates could be very high.

Contribution and results

Taking into account the components of a general reference architecture for UWSNs, we have analyzed [1] the total energy consumption of different principles for routing protocols in these networks — direct transmission, packet relaying and clustering — in two different scenarios: shallow water (depth lower than 100 m) and deep water (deeper ocean).

Our analysis has shown that the worst method is direct transmission, which exhibits bad results in the deep water scenario and is not recommended because it reduces the network throughput due to increased acoustic interference caused by high transmission power. The packet relaying technique results in energy savings in the deep water scenario and increases the network capacity; however, it also increases the complexity of a the routing protocol, and results in increased end-to-end packet delay. Routing protocols based on the clustering scheme [2] save more energy and exhibit a better performance in shallow water. Moreover, the clustering scheme is scalable with respect to the number of sensor nodes and the distance between them.

We have proposed the DUCS (Distributed Underwater Clustering Scheme) [3], a GPS-free protocol specifically designed for UWSNs. DUCS minimizes the proactive routing message exchange, and compensates the large propagation delays of the medium using a continuously adjusted timing advance, combined with guard times to minimize data loss and maintain communication quality. The effectiveness of DUCS has been demonstrated resorting to simulation.

Note: This work was carried out in collaboration with Universitat Politècnica de Catalunya

Bibliography

[1] M. Domingo and R. Prior, "Energy analysis of routing protocols for underwater wireless sensor networks," *Computer Communications*, vol. 31, no. 6, pp. 1227–1238, 2008.

[2] ——, "A distributed clustering scheme for underwater wireless sensor networks," in *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007*, 2007, pp. 1–5.

[3] ——, "Design and analysis of a gps-free routing protocol for underwater wireless sensor networks in deep water," in *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on*, 2007, pp. 215–220.

Body Sensor Networks - Uniting the Sensors

Pedro Brandão

In sensor networks, Body Sensor Networks (BSNs) encompass a particular set of restrictions and conditions that separate them from normal Wireless Sensor Networks (WSNs). More so than WSNs, BSNs would profit from different types of sensing information and the sensor network itself provides more opportunities for different applications to use the same resources. However, the heterogeneity of sensor hardware (HW) and the myriad of different applications that try to use them are an obstacle to its development. One current problem is the need to address specific characteristics of the HW without abstractions to provide the freedom to access the needed information while complying to a set of requirements. Our current research aims for a middleware approach that abstracts lower level details from applications. The approach envisions to use human models fed with data from the sensor network and query-able from the application layer. The main goals are to provide functionalities so that: a) applications are able to set requirements to be met on the information provided to them, b) several applications should be able to share the same resources, c) the resources should be optimized so as to meet the requirements and prolong the lifetime of the BSN.

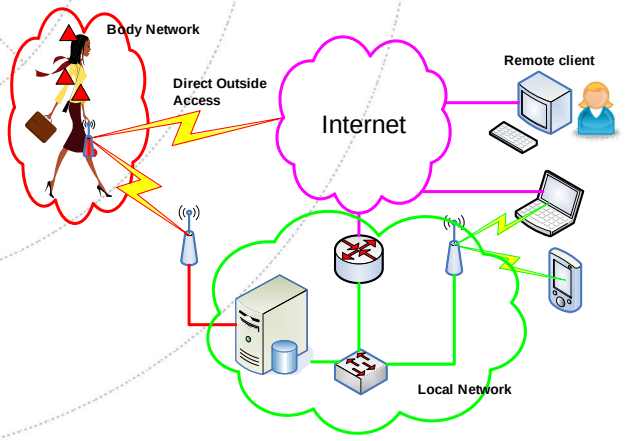
There is a need to abstract resources in Body Sensor Networks to enable correlation of different data and optimize resources.

Introduction

Healthcare monitoring and fitness assessment has led to the proliferation of sensor use for human body monitoring purposes. This can already be seen in commercial products for fitness assessment and several academic research initiatives for health monitoring.

As such there is a growing interest in a sensor network that lies within the *limits* of the human body [1]. There are several applications domains, be it monitoring vital signals of 1st responders and/or victims in disaster scenarios [2], health monitoring [3] (ranging from physical and chemical measures to video imaging or specific disease treatment (e.g.: diabetes). Deriving user context and performance are also scenarios dealt with BSNs, in one example force sensors are used to detect muscle work and correlate it with fatigue and freshness of users to derive recognition patterns.

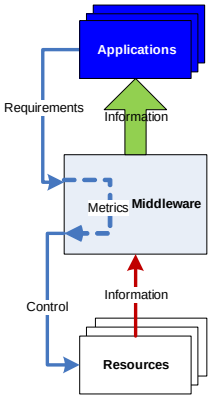
The general network view of BSNs is shown in *Figure 1*, where depending on the objective some of the networks may exist or not.



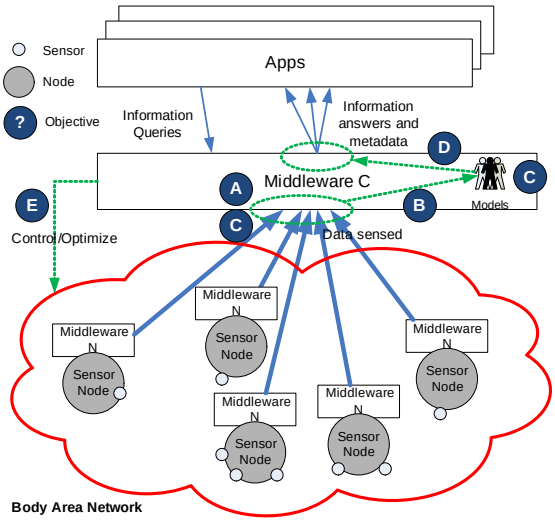
Networks in BSNs.

One issue that currently is not addressed in BSNs is the possible heterogeneity of available information. Most of the approaches deal with just one type of information or have find it complex to use different sources of sensing data. This would enable a better and more accurate estimation of the current situation through the correlation of different sensing information. As an example, blood pressure is more accurately measured when taking blood pressure, blood flow and oxygen levels. By adding an intermediate layer (middleware) to the process we could have: i) application requests blood pressure information; ii) middleware retrieves data from the available sensors (which could involve activating them); iii) middleware aggregates the available information using a defined model, adding metadata about the information (confidence on the value (based on the model and the data available), error margin (taking into account statistics of the sensors used), time of assessment, etc); iv) middleware provides to the application the information and metadata; v) application handles the

information taking into account its metadata. The application request could (and most likely would) have requirements associated.



Generic Architecture.



Architecture Proposed.

Our proposal is a middleware layer (portrayed in *Figure 2*) that abstracts the underlying BSN to the application, providing an information model to be queried. The information on the model itself is derived using the data provided by the BSN and applications state the models they want to use. Application requirements are mapped to resources metrics so that the middleware can optimize the resources while trying to fulfill the requirements.

General Architecture

The motivation for this proposal lies in the lack of an information abstraction to the sensor resources that copes with: i) collection and aggregation of sensor data to provide higher level information; ii) Metadata about the information derived; iii) compliance to application requirements; iv) management and optimization of resources. We introduce a middleware layer that provides the said abstraction and functionalities. The general middleware objectives are: **A)** collect data from sensor nodes; **B)** convert this data to relevant information in a human body model; **C)** collect metadata on the data received and correlate it to the information on the model; **D)** answer requests from applications based on the information in the model providing the related metadata; **E)** optimize resource usage (turn on/off, increase/decrease frequencies of data collection, etc) while complying to requirements set by the applications. *Figure 3* depicts this architecture.

Human Models

One of the interesting points with the problem at hand is related to the models to be used by the middleware. More specifically, how will the middleware map the data from the sensor network to the human model?

From a more complex mathematical formulation inherent in Mathematical Physiology to a tree like approach where different data with different weights is correlate to devise a higher abstraction the field is broad.

These models should nonetheless be framed such that the middleware is able to: i) unequivocally identify the information and its source; ii) infer commonalities between different models as to optimize resources and iii) clearly interpret how the metadata correlates in the model. Correlation of metadata information (error, rate, etc) should be part of the model.

Middleware

As stated, the middleware will deal with managing resources so to fulfill applications requirements. As seen in *Figure 3* 1 there will be parts running on the nodes (Middleware N) and the main block running on the central component (Middleware C). The responsibilities of both modules will be complementary so that information flows and control is attained by the main block.

The central component incorporates the optimization process, which is the most relevant component.

Finding a solution to maximize resource usage while satisfying application requests will mandate a definition of what are the requirements, metrics and controlled resources and how to map requirements to metrics so to optimize the said resources. We have already undertaken work on the first point where requirements (eg.: real time, data updates frequency, etc), metrics (eg.: QoS related, quality of measurement related, etc) and resources (eg.: network architecture, processing power, etc) have already been drafted. Optimization algorithms will play the relevant role in this issue.

Conclusion

Our proposal aims to release the BSN application developer from the details of the underlying HW by providing an abstraction to these resources, enabling the application to access the underlying information correlated and aggregated from the data provided by the BSN. Thus, applications can gain with data from different types of sensors (for the same or different types of information) without needing to address their specificities; applications can set requirements to be met in providing the requested information; several applications can more easily be accommodated on top of the same set of resources; resource usage can be optimized while taking into account the previous mentioned points; sensor plug-n-play capability can more easily be attained; compartmentalization of responsibilities provides better room for improvements/ updates (eg.: updating resource optimizations algorithms will not imply changes in applications). Applications can access higher level information based on a model that derives its values from the data on the sensor network.

This research is work in progress where the models (mapping between sensor data and model information) and the optimization of resources while meeting requirements are the main challenges. Other issues like network topologies and service discovery are also future work as the former will be related to resources and the latter with the ability to access information in a plug-n-play architecture. Experiments (healthcare and physical assessment) will be undertaken at a future point to test the proposed architecture.

Acknowledgements

This work results from joint research with Prof. Jean Bacon (University of Cambridge).

Bibliography

[1] G.-Z. Yang, O. Aziz, B. Lo, A. Darzi, B. A. Patel, C. A. Anastassiou, D. O'Hare, A. Radomska, S. Singhal, T. Cass, and H. Higgins, *Body Sensor Networks*, ser. User Interfaces, HCI and Ergonomics, G.-Z. Yang, Ed. Springer, 2006, vol. XXVIII.

[2] K. Lorincz, D. J. Malan, T. R. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: challenges and opportunities," *Pervasive Computing, IEEE*, vol. 3, pp. 16–23, Dec. 2004.

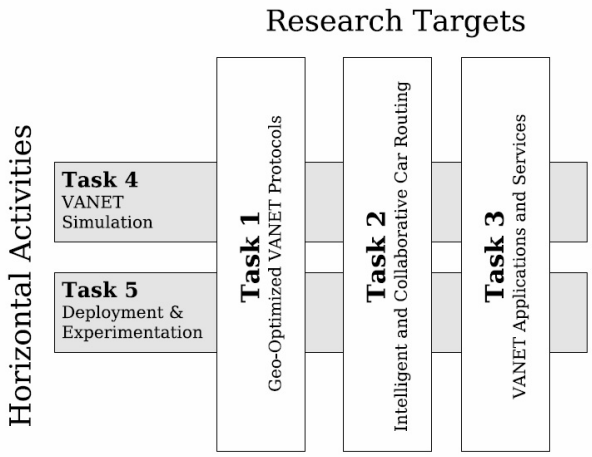
[3] I. Korhonen, J. Parkka, and M. V. Gils, "Health monitoring in the home of the future," *Engineering in Medicine and Biology Magazine, IEEE*, vol. 22, pp. 66–73, Jun. 2003.

DRIVE-IN: Distributed Routing and Infotainment through VEhicular Inter-Networking

João Barros, Michel Ferreira, Hugo Conceição, Rui Meireles and Mate Boban

The goal of the DRIVE-IN project is to investigate how vehicle-to-vehicle communication can improve the user experience and the overall efficiency of vehicle and road utilization. Vehicle-to-vehicle communication will be enabled by means of Vehicular Ad-Hoc NETworks (VANETs), a novel type of mobile ad hoc networks (MANETs) that has recently attracted significant interest from governments, academia, and industry, due to its potential to help save lives, increase the traffic efficiency, and provide a more pleasurable experience for drivers and passengers.

VANETs provide an opportunity for myriad of new applications, including location-based information dissemination, vehicle-based social networking and distributed interactive games.



Structure of the project.

1 Introduction

Up to now, vehicular navigation and communication were viewed as separate capabilities with little or no relationship to each other. A driver may for example communicate via telephone over a cellular network infrastructure and simultaneously use a Global Positioning System (GPS) navigation unit to find the fastest route to his destination; however, at the moment, the path he ends up taking is not likely to be a function of real-time information obtained via the communication network and the wireless transmitter usually does not exploit geographical information obtained from the GPS navigation unit.

Since the vehicle mobility and node density can vary dramatically depending on the road network and daily traffic patterns, it is important to explore how one can exploit the interplay between real-time navigation and wireless communication to achieve stable and efficient traffic and information flows.

2 Contributions

2.1 Geo-Optimized VANET protocols

The main objective of this task is to devise context-aware VANET communication protocols capable of leveraging the rich data sets provided by GPS receivers, such as position information, roadmap geometry, and traffic conditions, thus improving the utilization of the wireless medium and providing higher quality of service (QoS) for a wide range of applications. With this goal in mind, DRIVE-IN seeks for opportunities to use GPS data at every layer of the communications protocol stack. Fundamental transmission parameters, such as power, rate, and sender direction, can take into account the likely configuration of vehicles on the road. Likewise, the perceived vehicle density can be used to adapt the rules for wireless medium access. The network layer should ensure that information is routed not necessarily to one particular vehicle but towards the location where this information is most useful.

We shall compare the performance of our distributed car-to-car solutions with competing car-to-infrastructure alternatives, which require vehicles to communicate with cellular base stations or WiFi access points.

2.2 Intelligent and Collaborative Car Routing

This task targets the optimization of traffic flow through inter-vehicle communication. The current state-of-the-art of deployed traffic information sharing systems (e.g. TomTom HDTraffic) is

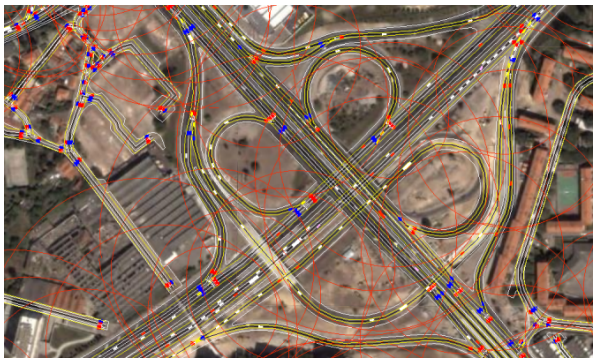
based on Floating Car Data, where cars act as sensors to collect traffic data and communication is based on a centralized client/server architecture. Penetration rate of such systems is very low which is one of the key reasons why simple centralized broadcast-based systems currently function: a limited number of vehicles can be routed efficiently by a centralized system using traffic data three-minutes-old, whereas a large number of vehicles could not be efficiently supported by such systems.
The approach of DRIVE-IN is based on traffic information sharing, as well as route information sharing, which is explored in a novel context of a mobile peer-to-peer (MP2P), short-range communication network. We propose to achieve a non-selfish, socially aware routing of vehicles through collaborative and intelligent navigation engines that implement spatio-temporal aggregation over past and current information, as well as over the shared planned routes, allowing an anticipatory avoidance of traffic congestions.

2.3 VANET Applications and Services

This task further relies on the foundational research in geo-optimized VANET protocols analyzed in Task 1, to propose, investigate and deploy challenging applications for inter-vehicular communication. In particular, we envision that the dynamic and interactive nature of VANET environment creates new opportunities for interaction between passengers in different vehicles, that we propose to explore in a novel scenario for multiplayer games. In order to determine the capability of VANET environment to support real-time applications, we analyzed the achievable QoS in such network [1]. Furthermore, we analyzed the stringent QoS requirements of multiplayer games and the required changes in the underlying game design [2]. The initial deployment on the prototype network of taxis (described in Task 5) will provide valuable feedback on the feasibility of different types of games over VANET. Furthermore, gameplay between passengers in different vehicles can also take advantage of some degree of planned route sharing, leveraging on work developed in Task 2.

2.4 VANET Simulations

Task 4, as a horizontal simulation framework activity, provides the necessary feedback from extremely complex scenarios to enable insights, identify critical problems, and test solutions throughout the project. This task spans the entire project, as it builds on our existing work, the DIVERT 1.0 simulator [3], that is being significantly extended. Wireless protocol design has to be closely articulated with the level of detail of the mobility and channel models used in the simulation framework. Continuous models, as opposed to discrete models which perform simulations in time steps, are able to capture much finer wireless connectivity information, that is particularly critical in VANET scenarios and applications.



VANET simulation

2.5 Deployment and Experimentation

Task 5 will provide a large-scale testbed for the three vertical tasks investigated in DRIVE-IN, by deploying the largest prototype VANET network to date, implemented on 500 to 1000 taxis in Porto. This large testbed will derive feedback impossible to obtain even with the most sophisticated simulation frameworks.

3 Conclusion

DRIVE-IN is a multidisciplinary project aiming to enable innovative traffic management, safety, and non-safety applications via the use of the largest VANET testbed ever deployed, as well as highly realistic VANET simulator. The project will yield novel geographically-aware routing protocols that will enable the aforementioned applications, and it will create new ways of exploiting traffic information, mobility of vehicles, and the behavior of the entire vehicular network to make the journeys safer, more efficient, and more enjoyable.

Acknowledgements

Joint Work with Profs. Ozan Tonguz and Peter Steenkiste from CMU and Prof. Susana Sargento from Univ. de Aveiro, IT.

Bibliography

[1] M. Boban, G. Misek, and O. Tonguz, “What is the best achievable QoS for unicast routing in VANETs?” in *The 3rd IEEE Workshop on Automotive Networking and Applications*, New Orleans, LA, USA, Nov 2008, pp. 1–10.

[2] O. Tonguz and M. Boban, “Multiplayer games over VANET: a new application,” *Ad Hoc Networks (submitted)*, 2009.

[3] H. Conceição, L. Damas, M. Ferreira, and J. Barros, “Large-scale simulation of V2V environments,” in *SAC ’08: Proceedings of the 2008 ACM symposium on Applied computing*. New York, NY, USA: ACM, 2008, pp. 28–33.

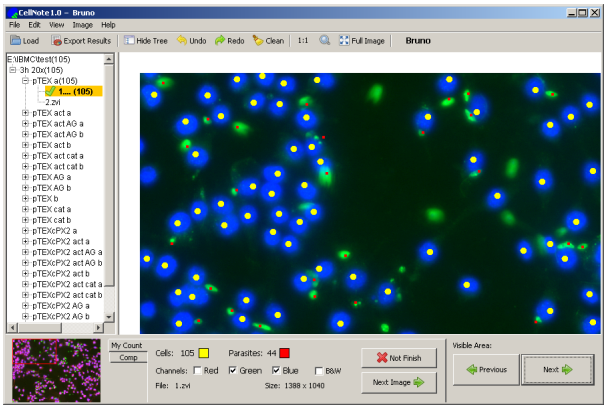
Software Platform for Assisted Analysis of Cellular Images

Bruno Lopes and Miguel Coimbra

Biology research laboratories such as IBMC (Instituto de Biologia Molecular e Celular) produce a large quantity of microscopy images that need to be analyzed. An example of an analysis is to count the number of cells and parasites in a given image to infer the infection level. In most situations, this analysis is performed entirely manually by the researchers themselves or by people hired specifically for this purpose. This manual analysis has some drawbacks: it is a slow procedure, since its made by humans, its prone to errors (by a number of factors such as counter's fatigue, stress, etc), and recounting is crucial for reliability of the analysis.

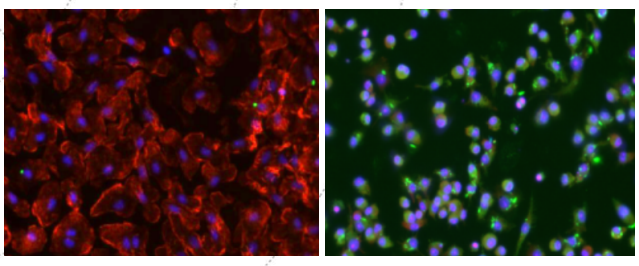
Another important factor in manual counting is that in some cases it can lead to seasickness of the person doing it, since he is looking at a moving scene, his brain process this information as if he is also moving but, another hand, getting in conflict with the signals from the inner ear, that's saying he is not moving.

To overcome these limitations it is necessary to eliminate the human factor, reduce the costs and the time spent in this kind of tasks. This can be achieved by automating the entire process. Therefore, the aim of this project is develop a software that it will analyze automatically a given set of cellular images.

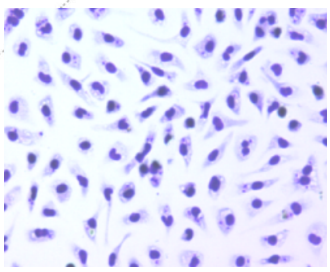


CellNote v1.0 - Manual Annotation Software

It has already been produced a software platform called CellNote v1.0 (Fig.1), in cooperation with IBMC, which is now used at this lab for supporting the manual annotation process of cells and parasites for Leishmania studies. Leishmania[1] is a parasite that affects man and dogs and that is present in many regions of the World, Portugal included. Infection by Leishmania may be fatal, but no satisfactory treatment is available. Determination of the level of parasite infection is a central tool in Leishmania research. This software has already enabled them to save time to manually analyze the images (Fig.2), but more importantly, it was possible to reduce the margin of error of the performed counts.



(a) Fluorescence Microscopy (b) Fluorescence Microscopy



(c) Giemsa Stain

Examples of microscopy images used for Leishmania research

Now, the next step is to design a software architecture to automatically process cellular images. In order to design a flexible and expansible software, the best solution is to have a design based on a modular architecture. This way, it can be used in a wide range fields of biological research and researchers would just plug the appropriate modules according to the their needs.

In the end, the user would only ideally need to indicate location of the images to process and output location to save the produced results, assuming that he has the appropriate modules. It would have the ability to automatically decide what is the more appropriate module to load a specific image. The results would be stored

in a central database so that data can be reused by other software, for example to produce a specific report.

This software will help improve the researchers' work by automatically processing and analyzing the experimental results, reducing the time and costs for this tasks, thus giving them more time to devote to do their research.

Acknowledgements

Joint work with Ana M. Tomás (Instituto de Biologia Molecular e Celular).

Bibliography

[1] http://www.who.int/tdr/diseases/leish/default.htm

Digiscope: DIGItally enhanced stethoSCOPE for clinical usage

Fábio Hedayioglu and Miguel Coimbra

In the ears of an experienced physician, a stethoscope yields important clinical information which can help an initial assessment of a patients clinical condition and guide the subsequent need for more specialized exams. This is particularly true in chest Medicine, i.e. Cardiology and Pneumology, which is the reason why the stethoscope still maintains a key position in Medicine in the modern era. Auscultation, however, is a hard skill to master. The heart sounds are of low frequency and the intervals between events are in the order of milliseconds, requiring significant practice for a human ear to distinguish the subtle changes between a normal and a pathological heart sound. The use of a digitally enhanced stethoscope, adequate for training physicians to improve their basic skills in diagnosing and treating heart conditions, or as a stronger tool for world-wide screening of specific heart pathologies are just some examples of how state of the art technology can be used horizontally to benefit people at different economical, political or geographical levels. This motivates the key objective of the DigiScope project: develop the prototype of a digitally enhanced stethoscope, capable of automatically extracting clinical features from the collected data, as well as providing a clinical second opinion on specific heart pathologies.

Figure 1: Stethoscope prototype developed by our research group.

The DigiScope project involves signal processing (clinical feature extraction), data mining (pathology detection using audio features and patient record information) and the ability to not only collect heart audio signals, but also to extract patient record information by communicating directly and efficiently with typically heterogeneous and complex hospital information systems.

Our published review [1] argues that the key to robust solutions lies in a stronger interaction with the clinical community, both for understanding the needs of cardiologists and robust clinical validation of the methods and of the final prototype.

Heart sound analysis is still an open problem

The main constituents of a cardiac cycle are the first heart sound (typically referred to as S1), the systolic period, the second heart sound (S2) and the diastolic period. Whenever a clinician is performing an auscultation, he tries to identify these individual components, and is trained to analyze related features such as rhythm, timing instants, intensity of heart sound components, splitting of S2, etc [2].

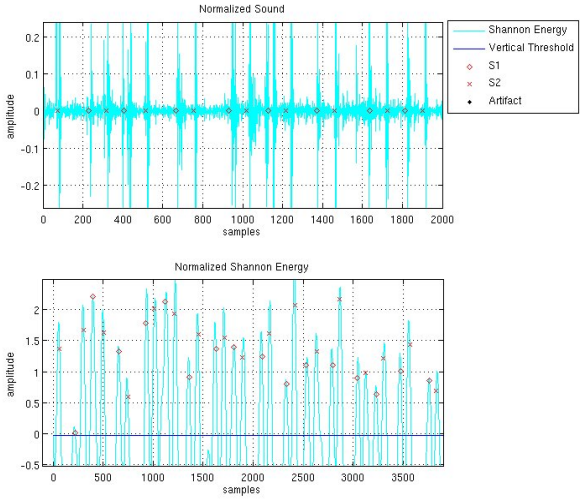


Figure 2: Example of sound segmentation.

This analysis allows him to search for murmurs and sound abnormalities that might correspond to specific cardiac pathologies. From a signal processing perspective, Heart Sound Analysis (HSA) is not only interesting by itself (allowing quantitative measures to be displayed automatically in a digital stethoscope), but it

is also an essential first step for the subsequent task of automatic pathology classification.

The vast majority of papers regarding cardiac audio processing, concern the detection of specific heart pathologies. This highlights the interest of the scientific community on this topic, but there are still some major flaws in most of them, such as the absence of a clinical validation step and unconvincing experimental methodologies.

Currently, an infrastructure composed by an integrated electronic patient record system, auscultation storage and retrieval system (all developed by our team), is running on the Royal Portuguese Hospital in Pernambuco-Brazil, having a team of physicians collecting patient data and auscultations and storing them on the IT's server. One M.Sc. thesis on heart sound segmentation is at the conclusion phase.

This project has a collaboration with Dr. Sandra Mattos from UMCF (Fetal and Pediatric Cardiology Unit) at Royal Portuguese Hospital in Pernambuco-Brazil.

Bibliography

[1] F. Hedayioglu, S. Mattos, and M. Coimbra, A Survey of Audio Processing Algorithms for Digital Stethoscopes, *Proc. of HealthInf*, 2009, Porto, Portugal.

[2] H. Liang, S. Lukkarinen, and I. Hartimo, A Heart Sound Segmentation Algorithm using wavelet decomposition and reconstruction, *19th International Conference - IEEE/EMBS*, 1997, Chicago, IL, USA

Body Signal Analysis for Monitoring Stress in First Responders

Ye Can and Miguel Tavares Coimbra

Clinical results suggest that physiological emergent events like heat stress and heart stroke, are predictable by physiological phenomena, such as fatigue and stress. It has also been shown that there are distinct fatigue and stress factors in First Responder Professionals, such as Fire Fighters (FF), Policemen (P) and Paramedics (Pm).

In the case of a fire event, fire fighters are very likely to be subjected to high temperatures. These might lead to Heat Stress (HS) and consequently cause heat related diseases such as Heat Strokes, i.e. the failure of human body's system of temperature regulation. In many critical situations, heat strokes are life threatening medical emergencies whose occurrence is very difficult to predict. Nowadays, based on body and environment temperature measures, inference of stress just from temperature values is possible.

The Vital Responder research project aims to explore innovative wearable technologies to provide secure, reliable and effective first-response systems in critical emergency occasions and develop biomedical solutions for diagnosis and monitoring support, with the emphasis on those physiological phenomena, such as fatigue and stress. More specifically, the goal of Vital Responder is to develop a wearable intelligent garment for monitoring and extracting vital physiological signals, like the electrocardiogram (ECG) and body temperature of Fire Fighters (FF), from those First Responder Professionals, such as Fire Fighters (FF), Policemen (P), Paramedics (Pm), who are also considered as the potential user of Vital Responder.

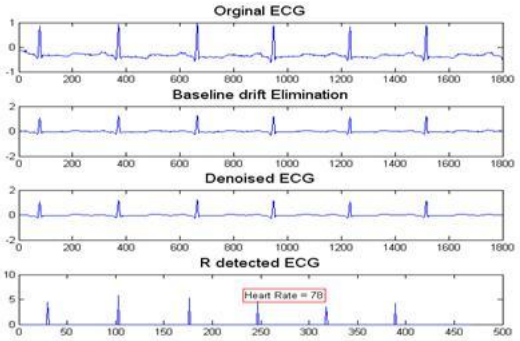
We also expect to deploy a telematic infrastructure that enables us to continuously monitor the collected information with a first focus on the detection of First Responder's stress. Extending further this idea, we are going to integrate the developed telematic system with an intelligent building system to better respond to emergency and critical events. By doing this, we also consider to explore wireless ad-hoc sensor network techniques to enable communication of vital signs and other parameters.

Consider the following scenario. Fire Fighters (FF) are monitored under the Vital Responder system within the fire event scenario (building, forest, etc). The intelligent garment firstly extracts the vital physiological signals and parameters, such as ECG, respiration rate, body temperature; the established wireless ad-hoc sensor network is responsible for transmitting these signals and other parameters like the location of FF elements to the developed telematic system at the terminal; relying on integrated telematic system, FF coordinator(s) or medical staff could monitor the healthy condition of FFs and respond to emergent cases.

The intelligent garment–Vital jacket

There is a worthy-noting innovative wearable technology-Vital Jacket, which is an intelligent wearable garment that is able to continuously monitor the electrocardiogram (ECG) wave, hence, allowing us to calculate the Heart Rate and monitor the electrical behavior of the heart. This information is quite significant in monitoring physiological health of a wide range of professionals, such as athletes at high performance sports and fitness. Real-time data obtained from Vital Jacket could be utilized in the preliminary research and analysis of ECG data, which is commonly used to measure stress in human beings and is therefore a key physiological signal in the Vital Responder system.

Currently, preliminary research has been started in the Vital Responder research project by exploring relevant public ECG data repositories, analyzing relevant papers and implementing relevant algorithms. This preliminary research would focus on the data analysis task, and would provide solid basis to achieve one of the main objectives of this project, which is the quantification of the effects of stress using signal processing and pattern recognition methodologies (specially in ECG signals). Furthermore, we expect that such research may lead to the automatic detection and



Example of an Electrocardiogram (ECG) Signal that can be monitored by the Vital Jacket.

prediction of critical stress situations, such as heat strokes in firemen.

Acknowledgement

This work results from joint research with Vijayakumar Bhagavatula, CMU.

Bibliography

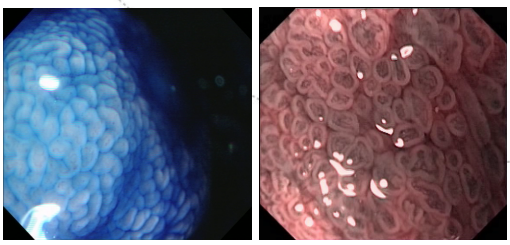
[1] Sahambi J.S., Tandon S.N., Bhatt R.K.P., Using wavelet transforms for ECG characterization. An on-line digital signal processing system, *IEEE Engineering in Medicine and Biology Magazine*, vol. 16, no. 1, pp. 77-83, Feb 1997.

[2] Cuiwei Li, Chongxun Zheng, Changfeng Tai, Detection of ECG characteristic points using wavelet transforms, *IEEE Trans. Biomedical Engineering*, vol. 42, no. 1, pp. 21-28, Jan 1995.

Computer Assisted Analysis of Narrow-Band Imaging Endoscopy

Farhan Riaz and Miguel Tavares Coimbra

Recent advancements in medical sciences have caused a steady decline in the number of reported deaths from gastrointestinal cancer, it is however still considered as one of the deadliest forms of cancer. This fact is attributed to the late detection of the disease, when it is already spread to the other parts of the body. The medical community, therefore, has felt the need to combine their efforts with computer scientists to fight this menace by devising systems, which can be used to screen the patients who have higher potentials of developing this disease in their lifetime. Different imaging technologies have been used so far to help develop Computer Aided Diagnosis (CAD) systems e.g. Virtual Colonoscopy, Chromo Endoscopy, Narrow-Band Imaging etc.



(a) Chromoendoscopy (b) Narrow-Band Image

It is our objective to investigate the potential of the Narrow-Band Imaging technique in order to diagnose cancer in the patients. NBI uses two discrete band of light (Blue and Green), which is considered to enhance the vascular structures in the gastrointestinal tract. Since this vascularity is considered as an important factor to reach a final decision about diagnosis, therefore, we aim to devise a CAD system which can detect vascularity patterns and hence, assist the doctors in reaching a decision about diagnosis. In addition to vascularity, the regularity of the pit-patterns is also considered an important factor for diagnosis. This regularity is easily detectable using other technologies like chromo endoscopy which are widely used for diagnosis, therefore in the first phase of this thesis; we have performed a state-of-the-art work on chromo endoscopy. The chromo endoscopy images were obtained using an endoscope at the Portuguese Institute of Oncology (IPO). The physicians annotated about 144 images and they were used as our ground truth data to evaluate the performance of segmentation algorithms.

In medical images, the doctors do not consider the whole image as relevant. They consider some parts of the image in order to reach a decision about the diagnosis and, therefore, it makes sense to perform a segmentation of the images to find parts of the images which are clinically relevant. We used Mean Shift (MS) and Normalized Cuts (NC) based on their success and popularity for segmentation of medical images. The segmentation results yielded by these methods were then compared with the manual annotations of the same images made by specialist doctors. We used five different measures, which were considered to be important for this type of comparison. The criteria for selecting them were based on the fact that the segments obtained from these algorithms should lie as much as possible inside the annotated areas because if this is not the case, our system uses the image segments which were not clinically relevant, hence leading to a wrong diagnosis. Five measures, which we used for this purpose are:

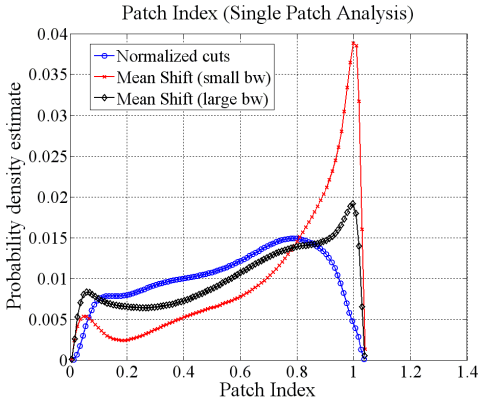
- Number of Patches
- Patch Index (Percentage of segment lying inside segment)
- Annotated Area Covered
- Euclidean Distance of Point Correspondences (Shape)
- Dice Coefficient

These measures take into account over/under segmentation, area similarity and shape similarity of the annotated and segmented contours.

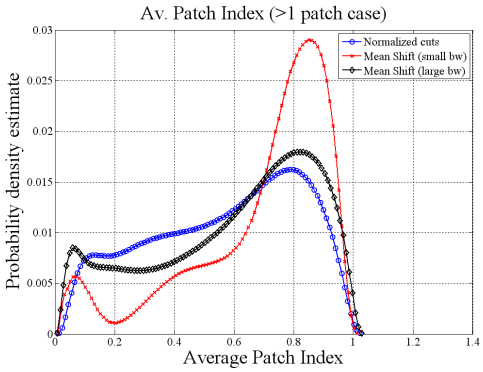
We found in our results that when using only a single image segment for doing diagnosis, NC performs better. MS is a parametric method and hence, if a smart solution for selection of the parameters is made, MS can theoretically perform better as compared with NC (we used fixed parameters for MS). If, however, we have a system which can make use of more than one image segments to approximate the annotated area, MS is a better choice.

Acknowledgement

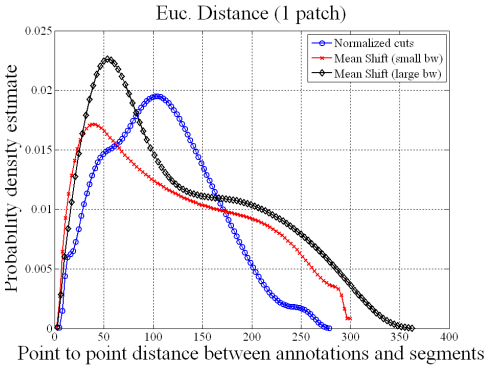
This work results from joint research with Mário Dinis Ribeiro, Cintesis.



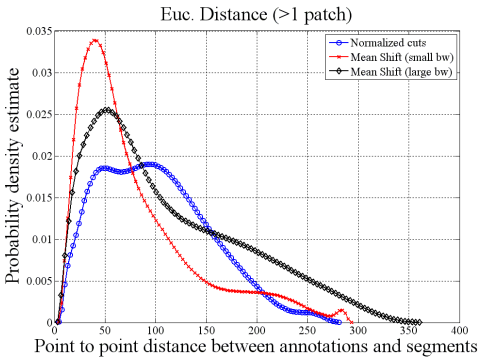
Patch Index - Single Segment



Patch Index - Multiple Segments



Point Correlation - Single Segment



Point Correlation - Multiple Segments

Bibliography

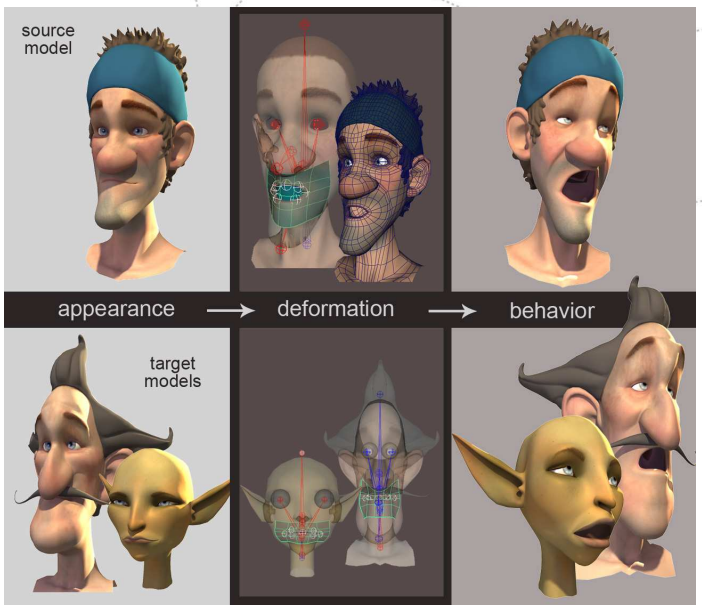
[1] D. Comaniciu and P. Meer, “Mean Shift: A Robust Approach Toward Feature Space Analysis”, *IEEE trans. Pattern Analysis and Machine Intelligence*, vol. 24, no. 5, pp. 603-619,May 2002.

[2] J. Shi, J. Malik, “Normalized cuts and Image Segmentation”, *IEEE trans. Pattern Analysis and Machine Intelligence*, vol. 22, no. 8, pp. 888-905, Aug. 2000.

A System to Reuse Facial Rigs and Animations

Verónica Costa Orvalho

Facial animation in films and videogames are strongly dependent on a fixed rig that is custom created for each character. The rig is defined in the early stages of the development and is conditioned by the characters morphology. We present a portable character rigging system that integrates into current animation production pipelines enabling digital artists to create more lifelike characters in less time about 90-99% faster, when compared to traditional animation techniques. It automatically transfers the rig and animations created in one character to different characters, independent of their shape and appearance. Artists are not forced to use predefined rigs and can preserve the original mesh they created. As a result, the system improves the workflow in CG productions, the modeling and animation teams can now work in parallel.



Overview: define the source and target model; adapt the source model geometry to fit the target; transfer attributes and shapes; bind the influence objects and skeleton to the target. The result is a model ready to be animated. (Copyright 2005 Dygrafilms)

Introduction

Facial animation presents many difficulties (time, cost and complexity constraints) that limit its adoption and usefulness in different situations. *Pighin et al.* [1] discuss the research efforts and main challenges faced by some blockbuster films, and emphasize that facial puppetering and the use of nonlinear rigs are still unexplored issues. Generating realistic face movements is hard, because even with current 3D software, animators cannot capture and control every detail of the face. To obtain the desired realism, traditional animation pipelines have each character separately rigged by hand, a very labor-intensive and time-consuming task. A rig is a set of controls that allows an artist manipulate a character. The character rigging process is analogous to setting up the strings that control a puppet, which in the hands of an experienced digital artist comes to life [2]. Finding a technique that provides accurate and fast rigging remains a challenge. Our solution overcomes this problem because it adapts the inner structure of the characters to the shape and facial features of the models. Artist can always keep the mesh they created, so the visual look of the characters is never affected. This is fundamental to guarantee the high quality results required by the entertainment industry (e.g. Playable Universal Capture *Borshukov et al.* [3]), which allows creating and reproducing animations that respect the style and expressiveness of each character, making them unique. Previous methods [4, 5, 6] do not deal directly with the artists needs, and most are oriented towards human look. Our approach is general, so artists can define their own rig and then quickly apply it to different models, even with disparate proportions and appearance (human, cartoon or fantasy). This gives artists complete freedom to manipulate the characters: they can create new animations and not be limited by pre-generated ones. The system we present can easily be integrated into current production pipelines as it is embedded in Maya (Autodesk 2008 [7]). The technology behind the system is described in Orvalho PhD Thesis [8]. It also includes an extensive state of the art analysis related to MPEG-4, FACS another animation techniques. Figure 1 shows an overview of the system.

Related Work

Facial animation re-targeting between dissimilar meshes is not a new problem, but facial rigging re-targeting still unexplored. Most work deals only with the geometry of the face and forgets that the key elements to animate a character is the structure underneath the 3D model mesh. Our work differs from previous approaches that focused on transferring animations, because we aim to transfer the complete facial rig, in addition to animations. We also want to allow the reuse of a facial rig in different face models, regardless of the type of the rig. Thus, most existing work is not efficient for real-time animation, are to complex to setup, force the artist to use a fix pre-defined rigs and there is no previous work capable of dealing with our variety of morphologies [9].

Many efforts have been done to re-target or automatically create the body rig of characters [10, 11] and achieved good results, but none have focus on facial rig re-targeting. Most facial animation is related to *physically-based*, *geometric deformation* and *performance-driven* methods.

Physically-based methods K. Kahler et al. [12] simulate the contraction and relaxation of human muscles to animate faces. *Yuencheng et al.* [13] used a multiple-layer dynamic skin and muscle model, together with a spring system, to deform the face surface. But these techniques make it hard to define accurate muscle parameters, due to the complexity of human muscles. So, *Sifakis et al.* [9] used non-linear finite element implementation to determine accurate muscle action, captured from motion of sparse facial markers. The method shows the success of performance-driven animation, but it is not clear if it can handle anatomically inaccurate models.

Geometric deformation methods use a variety of techniques to animate faces. Following *Sederberg and Parry* [14], *Chadwick et al.* [15] used Free-Form Deformation (FFD) for layered construction of flexible animated characters, which doesn't require setting the corresponding features on the geometries. *Turner and Thalmann* [16] used an elastic skin model for character animation. Other approaches were introduced for high level geometric control [17, 18] and deformation over 3D model, to help simulate wrinkles [19, 20]. These deformation methods provide artists with easy controls to generate animations, but automating these procedures still needs considerable effort.

Performance-driven methods [3] capture the facial performance of an actor, which can be re-targeted to different face models [21, 22] or blendshapes [5]. These techniques can generate realistic facial motion, but are expensive to use. Also, they are more suited for human beings than imaginary or fantastic characters.

Facial Rigging Challenges

"Rigging is the process of taking a static, inanimate computer model and transforming it into a character that an animator can edit frame-by-frame to create motion" [23]. The result is a rig that can be manipulated by a set of controls like a virtual puppet [24] or by motion capture data. Creating the character rig is a very complex, time consuming and labor intensive task. Still, there is no defined standard methodology for rigging a face. Studios continue to redefine the techniques, processes, technologies and production pipelines to efficiently create films and videogames.

Today, facial animation is done manually by skilled artists, who carefully place and manipulate the animation controls to create the desired motion. As models become more and more complex, it is increasingly difficult to define a consistent rig that can work well for many different characters. So each facial rig has to be created individually by hand. This traditional method ensures high quality results, but it is slow and costly. Large film and videogame companies can afford hiring lots of artists, but this is not feasible for low budget production. It takes an experienced digital artist from one to four weeks to create a complete facial rig, depending on its complexity. But if any change must be applied to an already created rig , the rigging process has to restart. Facial rigging becomes a serious bottleneck in any CG production.

Finding the optimal solution to create a facial rig depends on several constraints: time to develop the rig, budget, artists'experience, expected rig performance and actions, and others. The three most common approaches to create a rig are based on: blend shapes [25], bones [26] or a combination of both [17]. However, there are other existing facial animation methods, like motion capture, that can produce photo-realistic results and speed up the animation process, but are unable to adapt the performance to dissimilar characters. The captured animation will look the same in all models, ignoring their different appearances. Motion capture focus on analyzing what data to transfer, while our approach focus on what data to transfer and how to represent it.

Thus, the uniqueness of faces makes facial synthesis so challenging. The smallest anomaly in the face shape, proportion, skin texture or movement is immediately detected and classified as incorrect. Most rigging challenges are:

- **no standard:** artists do not follow a formal criteria or methodology when creating a rig, making it difficult to create a solid platform to build upon;
- **changing the geometry or resolution:** it is very common to change the face model during production, to improve the deformation details or simply because it looks better. Any minor modification in the model surface (a bigger nose, more resolution around the lips) after the character is rigged, causes the rigging process to restart;

- **reusing weight maps:** the weight distribution defined for one character will not work on others.
- **number of shapes leads to complex user interface:** many productions use rigs based on hundreds of shapes. Usually, too many shapes make it hard to use the rig. Likewise, if a shape is added during production it can generate two problems: the shape conflicts with existing animations, making it necessary to rework some shots; or the new shape does not mix nicely with the the others;
- **preserving a consistent look:** placing by hand the animation controls leads to different artistic interpretations of where to position each element of the rig. This makes it difficult to easily reproduce the same facial pose between different characters. Consequently, it becomes hard to guarantee a consistent look throughout the production;

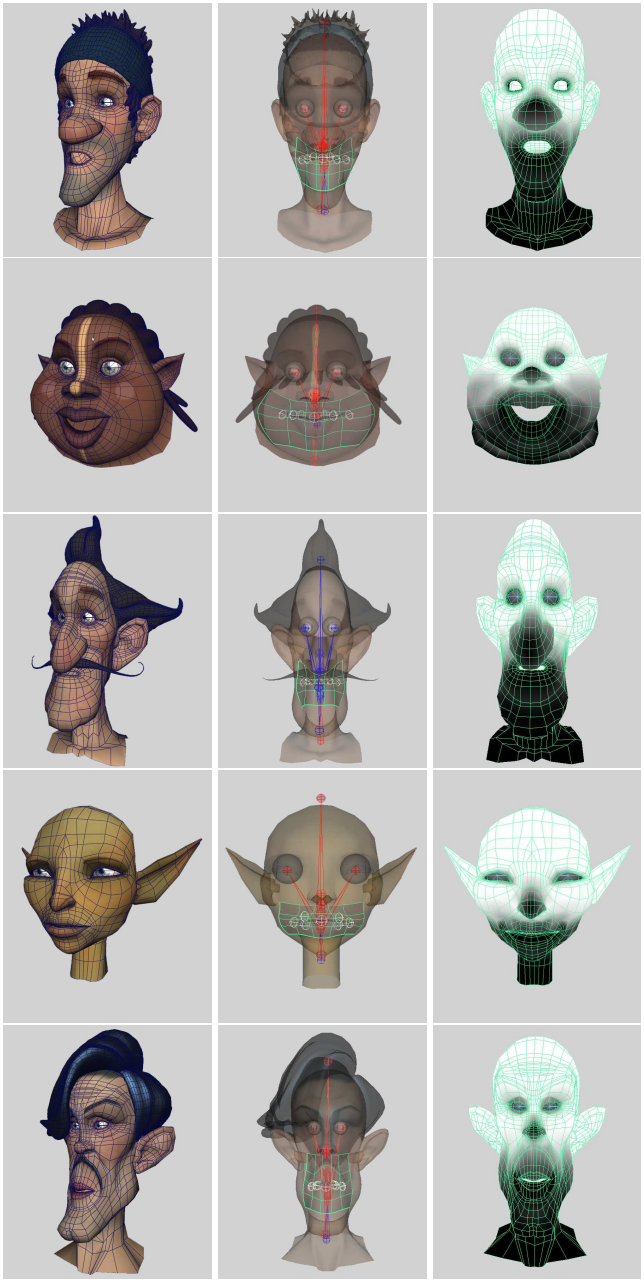
Our Facial Rigging System

Creating and placing by hand each component of the rig (bones, controls) quickly becomes impractical when complexity grows. The system we present can handle simple and complex rigs based on a new approach described in our previous work [8]. The system is:

- **generic:** the facial rig can have any type of configuration and does not force the use of a predefined rig;
- **flexible:** the rig has no initial constraints;
- **independent of the shape:** a facial rig can be transferred between models that have different geometry, look and appearance;
- **enhances artistic freedom:** artists can use any tool or deformation method to create the rig.

System Description

The system deals with the setup of the character rig. It allows using the rig created for one character in others. To transfer the facial rig we begin by defining two 3D face models. The first one, we call source model, is rigged and includes a series of attributes: a control skeleton, a number of influence objects that represent the inner structure of the face and animation controls, facial expressions (shapes) and animation scripts. The rig doesn't have initial constraints and can be created by an artist. The second model, we call target model, doesn't have a character rig associated to it. The source and target models can have different descriptors: one can be defined as a polygonal surface and the other as a NURBS surface. Also, the faces do not need to have the same number of vertices. Figure 1 shows an overview of the system pipeline and illustrates the rig transfer process with two dissimilar characters.



The first row shows the source model (Lisandro) and the rest show the target models (Mostaza, Teseo, Hada and Demetrio); first column shows the look and appearance of the models; second column details the facial rig that includes 21 joints and 1 NURBS surface; and third column shows the weight distribution. All models have different wireframe. (Copyright 2005 Dygrafilms)

The main steps within the system are: 1. surface deformation; 2. attribute transfer; 3. skinning.

1. Surface Deformation The source rig information is used as the direct input for transferring the setup to the target model. First, our deformation method deforms the source model surface to match the geometry of the target. We landmark the facial fea-

tures to keep correspondence between source and target model, and then employ a computer vision interpolation technique named Thin Plate Splines (TPS) [27], as our deformation kernel function. After the TPS, the source surface only has exact deformation at the landmark positions of the target model, while the rest of the points lay outside the target surface. We solve this by applying a dense correspondence algorithm [8], which projects every point of the warped surface to the closest point of the target and determines the correspondence between every source and target vertex.

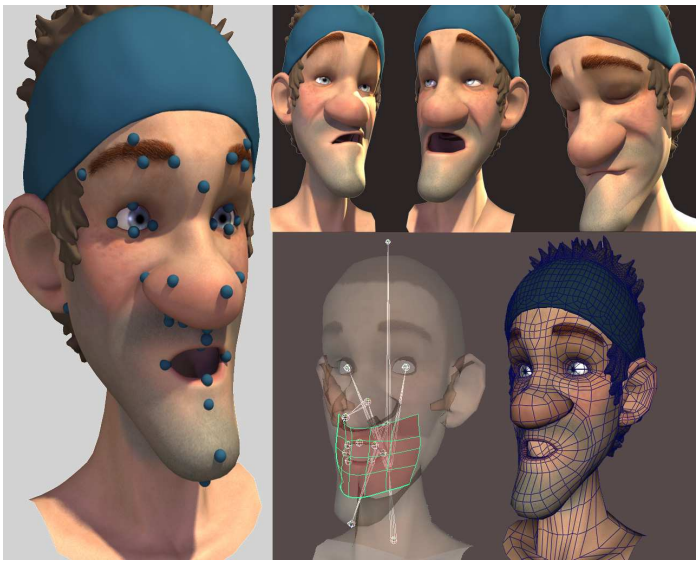
2. Attribute Transfer Using as reference the previously deformed source surface, we call guide model, the method accurately places the source rig attributes (section describes the rig attributes) into the target model, even if they have different geometric proportions. We had to adapt the TPS to properly deal with each attribute specific characteristics. It is not the same transferring bones than transferring a NURBS curve. The dense correspondence avoids placing additional landmarks on the influence objects or on the skeleton structure. The deformation process achieves excellent results in positioning the source rig attributes in the correct regions of the target face. For example, joints and NURBS surfaces are relocated in the target model, based on the correspondent position they have in the source model. They are also transformed to fit the shape and size of the target (see figure 2).

3. Skinning After the deformation step comes the skinning, based on a smooth binding algorithm. It binds the transferred attributes to the target model using the adjusted weights of the source, avoiding the need for manual weighting. The weights at the target are calculated using the deformation method. Each vertex of the target model accurately adapts the blending weight of the joints and influence object, based on the source model weight distribution, to properly represent the target facial look and behavior (see figure 2). Last, as the target model is already rigged and weighted, transferring facial animations is a straightforward process. The method only needs to scale and adapt the animation curves to fit the proportions of the target. The end result are face models ready to be animated with production quality rigs.

Rig Definition

Central to our system is the notion of source rig $\mathcal{S}$, and we use the model in figure 3 to illustrate it. The rig is formed by different layers of abstraction that we refer to as attributes: skin surface $\mathcal{S}_S$, influence objects $\mathcal{S}_O$, skeleton bones $\mathcal{S}_B$, facial features landmarks λ, shapes $\mathcal{S}_H$, animation scripts $\mathcal{S}_A$ and other components for representing the eyes, teeth and tongue. We can assign additional attributes to each of these layers: weight, texture, etc. [28].

The source rig helps define the appearance of the characters. It establishes the character setup standard shared by all the models. Artists can create their own source rig, because they are free to use any type of controls and components to achieve the desired visual look.



Source rig used in our examples; images show different rig attributes: landmarks, expressions (created using the rig and shapes), joints and NURBS surface, wireframe. (Copyright 2005 Dygrafilms)

The **source rig** $\mathcal{S}$ has been modeled manually and is a highly deformable structure of a face. During the modeling process, we used facial features and regions to guarantee realistic animation and reduce artifacts.

The **surface** $\mathcal{S}_S$ is the external geometry of the character that determines the skin of the face, using polygonal surfaces composed by a set of vertices **r** and a topology that connects them.

The source rig is tagged with **landmarks** λ, distributed as a set of sparse anthropometric points. We use the landmarks to define specific facial features to guarantee correspondence between models.

The **skeleton** $\mathcal{S}_B$ is a group of bones positioned under the skin. It defines the pose of the head and controls lower level surface deformation. Each bone is defined by two joints, one at each end of the bone.

The **influence objects** $\mathcal{S}_O$ are objects that affect the shape of the skin and help artists control the 3D models. They include: NURBS surfaces, NURBS curves, lattice deformers, cluster deformers, polygon mesh, and others.

The **shapes** $\mathcal{S}_H$ are new 3D face models created by applying deformations over the geometry $\mathcal{S}_S$ of the character. A shape is a 3D facial pose of the source model, where $\mathcal{S}_H$ and $\mathcal{S}_S$ have the same geometry. Shapes are usually modeled manually by an artist. They represent facial expressions or partial deformation of a specific area of the face. They are used to create blend shapes, which let you change the shape of one object into the shapes of other

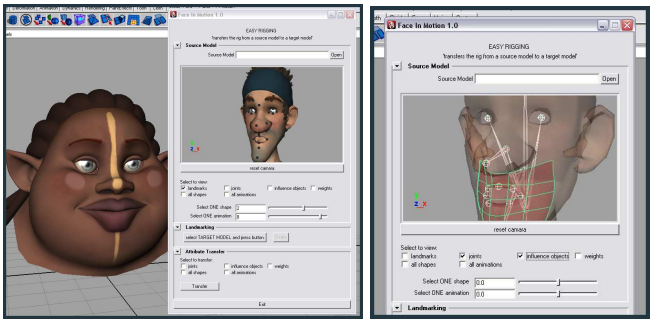
objects. The interpolation between shapes results in facial animations.

The **animation scripts** $\mathcal{S}_A$ consist of a list of animation curves that determine motion. Each animation curve represents changes in the value of an attribute, like shapes or bones.

Application and Workflow

We implemented a set of plug-ins in C++ for Maya [7]. The plug-in includes a simple user interface to ease the landmarking and assist the transfer process (see figure 4). The modular design of the application makes it simple to integrate into existing animation pipelines.

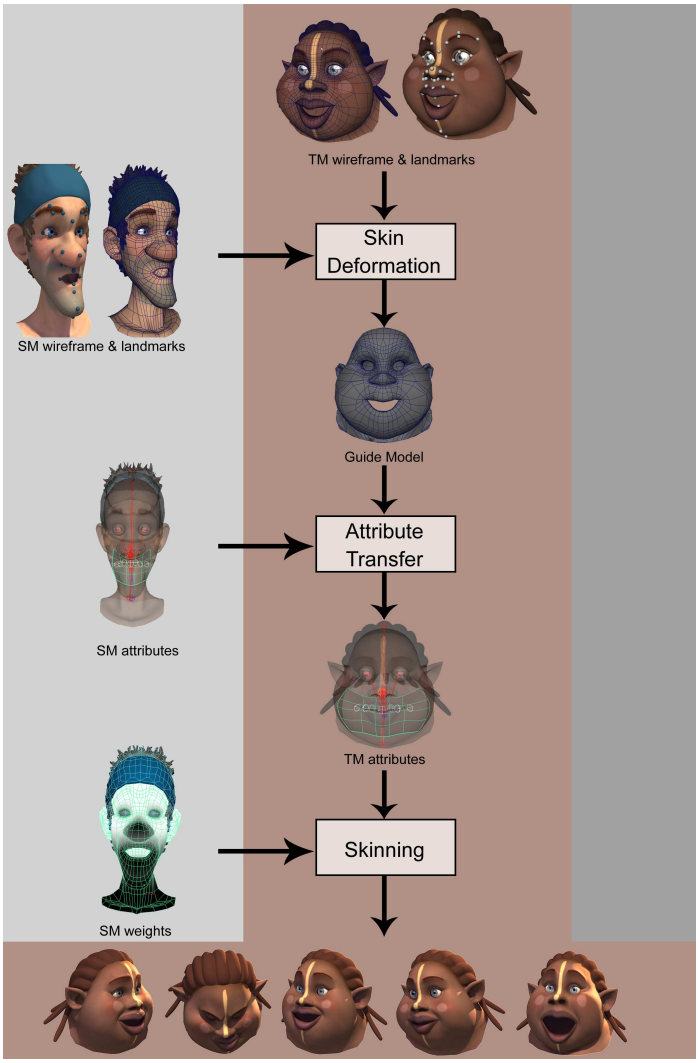
The application enables artists to fit automatically the rig from the source to the target model; manipulate the target as if they were using a puppet; and adjust animation parameters in the target model or animate the target using predefined source animations.



Application user interface running on Maya: assisting the landmarking process (left); close up of the source rig viewer with joints and influence object selected (right). (Models copyright 2005 Dygrafilms)

The *input* to the pipeline is the source model $\mathcal{S}$ information. The *output* is a fully rigged target model $\mathcal{T}$ ready to be animated. The workflow of the application is as follows:

1. **Landmarking**: Defines the source and target model landmarks that will keep correspondence between models.
2. **Surface Correspondence:** Ensures the exact point matching at the landmarks and smoothly interpolates the deformation of other points.
3. **Surface Dense Correspondence:** Ensuring exact deformation of every surface point, avoids placing additional landmarks.
4. **Attribute Transfer:** Uses the TPS deformation method to transfer each type of attribute.
5. **Skinning:** Binds the deformable objects, influence objects and surface to the skeleton of the target model.



System pipeline. Shows the three main steps needed to transfer a facial rig: skin deformation, attribute transfer and skinning. The output of the skin deformation is the guide model, which serves as reference for the rest of the transfer process. The output of the attribute transfer is the target model with the rig components positioned in correspondence to the source. Last, after skinning the character using the source model weights, the target model is rigged and ready to be animated. (Copyright 2005 Dygrafilms)

Results and Discussion

Reproducing the subtleties of a face through animation requires developing a sophisticated character rig. But, creating by hand the inner structure and controls of each character is a very labor-intensive and time-consuming task. We presented a system that transfers the rig and animations between characters, at least an order of magnitude faster than traditional manual rigging. The system allows *creating* the rig, animation controls and scripts for *one model* (source), and *reuse* them in many different *target mod-*

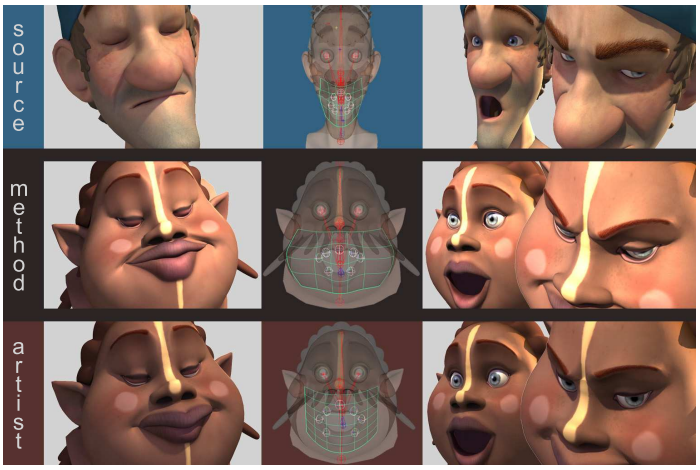
els. It is independent of the appearance or shape of the model, so rig transfer between dissimilar characters is feasible. Artists can create their own rigs and are not forced to use predefined ones. In film and videogame productions, artists are often given one base model to make all new faces (shapes). Also, it is common that afterwards they are asked to use a different 3D face, because it has improved deformation details or simply looks better. Currently, all shapes need to be remade to reflect the topology of the new face. But our method makes sure that previous work can be transferred and artists time is not wasted.

Our facial animation system can be integrated into existing animation production pipelines, improving its work flow as it decouples the work of the animators and the modelers, they can be working in parallel on the same character. As a result, the companies will have fewer bottlenecks, which will increase productivity and reduce cost.

The system also provides a solid foundation for setting up consistent rigging strategies: at the beginning of a production, artists can define the required rig parameters and afterwards use them as a template for all models. This rig becomes the building block for all characters. Our approach helps film and videogame studios overcome the current lack of a standard rigging methodology. It guarantees that all rigs generated by the system produce homogeneous results, ensuring that the models share a common vision and consistent artistic style.

Testing and Validation We validated the system with a series of experiments. We used source models from several companies (Electronic Arts, Blur Studios, Dygrafilms, etc.) and for each, we transferred the rig and animations to different target models. We worked with a variety of styles: human, cartoon and fantastic creatures. Then, for the same models, we compared the output of our application with the results manually created by an artist. The results were supervised by Technical and Art Directors, who approved the quality of our rig and animations to be used in CG productions, replacing the artist generated ones (see figure 6 for a detail explanation). This is a crucial result: if the output still requires a lot of tuning, then the system is useless in a production. The examples of the paper are limited to synthetic characters to emphasize the versatility of the method.

Performance Our application allows creating the rig in one hour as we need to visually validate the results, (go through all the rig) which take some time if the rig is very complex. The attribute transfer process like changing the weights, modifying a control position or transferring animations, is nearly instantaneous. Figure 7 shows that our method convincingly captures the complex effect of simulating a talking head, to be used in a film. The big time savings achieved on the rigging process is usually an order of magnitude or more, and still meet the high quality animation needs of the entertainment industry. The tests were made on a AMD Athlon 64 3500+ CPU with 2 GB of RAM.

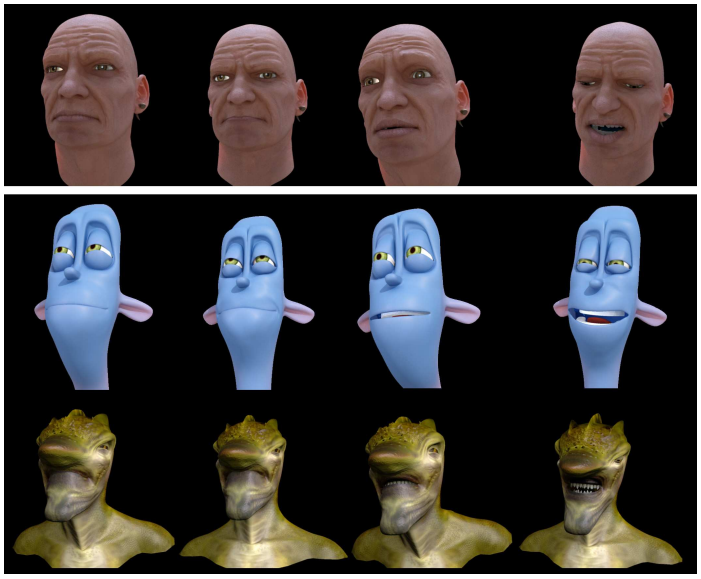


Comparison of the target models automatically generated by the method and manually created by an artist. The images on the middle show a NURBS surface that simulates the orbicularis mouth muscle: we can see that the method is more precise than the artist when adapting it to the target geometry. This is a particularly difficult task for the artist; he has to make sure that the NURBS parameters are homogeneous to avoid strange deformations or artifacts in the mouth (like pinching in the lips). This is a also an example of transferring animations between dissimilar geometries: the method preserves the intensity of the facial expressions and animations of the source. (Copyright 2005 Dygrafilms)

Source (1st row) and target models (2nd and 3rd row) animation sequence: frames from a video that integrates facial animation with lypsync. (Copyright 2005 Dygrafilms)

Extreme Test To test the method to the extreme of its possibilities, we ordered three very different 3D models: a photo-realistic human (source model), a cartoon and a fantastic creature (target models). The models differ enormously in artistic style, deformation behavior, shape and proportions (see figure 8). The source model rig includes: 2 NURBS curves around the mouth, 1 lattice for the jaw, 6 joints for the head, 5 joints for the tongue, 3 joints for the teeth, 47 shapes and 2 animations clips (one with

extreme facial poses and the other with lip-sync). The method successfully transferred the shapes in the mouth region, which is very complex due to the variety of poses it can perform. But the drawback of transferring shapes between characters with different styles is that the target models inherit the movements of the source. We obtained a cartoon model simulating a human character. This faithfulness it is not always what the artist wants, so we needed to keep in mind this behavior.



Source (top) and target models (bottom). Keyframes extracted from a video sequence to show different poses transferred from the source to the target models. The poses were created by manipulating the source rig. (Copyright 2007 Face In Motion)

Limitations An important issue to mention is that if the source rig quality is low, the transference is still successful but the results on the target will be of comparable quality. The technology is indeed independent of the quality and the shape of the rig. During our tests, we realized that when the source model has the eyes and the mouth completely closed, the attribute transfer results show some artifacts. This a current limitation of our solution. To obtain artifact free transfers, it is recommended to have the eyes and mouth of the source and target models slightly opened.

Future Work We performed some tests on mapping motion capture data into the source rig, and later transfer it to the target model. This is an interesting direction for future research and to extend our application.

Acknowledgement

Many thanks to Juan Nouche (Ottiplanet) and Xenxo Alvarez (Enne Studios) for their feedback and for providing the 3D models while working at Dygrafilms. Also to Fred Fowels (Rainmaker), Jean Luc-Duprat (Intel) and Crystal Wang (Electronic Arts) for testing the system and providing 3D models and motion capture data. Special thanks to Toni Susin for supervising the research project. Last, we would like to thank Blur Studios for using our system into their CG pipeline to create the facial rig of the Simpsons and Fable productions. This project is partially funded by FCT, Portugal (`http://www.it.pt`).

Bibliography

[1] F. Pighin and J. P. Lewis, "Facial motion retargeting," 2006, in SIGGRAPH'06: ACM SIGGRAPH Courses, ACM Press, New York, NY,USA.

[2] K. Richie, O. Alexander, and K. Biri, "The art of rigging vol. 2," 2005, cG Toolkit.

[3] G. Borshukov, J. Montgomery, and W. Werner, "Playable universal capture: compression and real-time sequencing of image-based facial animation," 2006, in SIGGRAPH'06.

[4] J. Noh, "Facial animation by expression cloning," Ph.D. dissertation, Los Angeles, CA, USA, 2002, adviser-Ulrich Neumann.

[5] Z. Deng, P. Chiang, P. Fox, and U. Neumann, "Animating blendshape faces by cross-mapping motion capture data," 2006, ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games (I3DG06).

[6] K. Wampler, D. Sasaki, L. Zhang, and Z. Popović, "Dynamic, expressive speech animation from a single mesh," in *SCA '07: Proceedings of the 2007 ACM SIGGRAPH/Eurographics symposium on Computer animation*. Aire-la-Ville, Switzerland, Switzerland: Eurographics Association, 2007, pp. 53–62.

[7] I. AUTODESK, "Autodesk maya," 2008, http://www.autodesk.com/maya.

[8] V. C. Orvalho, "Reusable facial rigging and animation: Create once, use many," Ph.D. dissertation, Barcelona, Spain, 2007, adviser-Antonio Susin.

[9] E. Sifakis, I. Neverov, and R. Fedkiw, "Automatic determination of facial muscle activations from sparse motion capture marker data," *ACM Trans. Graph.*, vol. 24, no. 3, pp. 417–425, 2005.

[10] I. Baran and J. Popović, "Automatic rigging and animation of 3d characters," in *SIGGRAPH '07: ACM SIGGRAPH 2007 papers*. New York, NY, USA: ACM, 2007, p. 72.

[11] C. Hecker, B. Raabe, J. Maynard, and K. V. Prooijen, "Real-time motion retargeting to highly varied user created morphologies," 2008, in SIGGRAPH'08.

[12] K. Kahler, J. Haber, H. Yamauchi, and H. P. SEIDEL, "Head shop: generating animated head models with anatomical structure," 2002, in SCA'02.

[13] Y. Lee, D. Terzopoulos, and K. Walters, "Realistic modeling for facial animation," in *SIGGRAPH '95: Proceedings of the 22nd annual conference on Computer graphics and interactive techniques*. New York, NY, USA: ACM, 1995, pp. 55–62.

[14] T. W. Sederberg and S. R. Parry, "Free-form deformation of solid geometric models," in *SIGGRAPH '86: Proceedings of the 13th annual conference on Computer graphics and interactive techniques*. New York, NY, USA: ACM, 1986, pp. 151–160.

[15] J. E. Chadwick, D. R. Haumann, and R. E. Parent, "Layered construction for deformable animated characters," *SIGGRAPH Comput. Graph.*, vol. 23, no. 3, pp. 243–252, 1989.

[16] R. Turner and D. Thalmann, "The elastic surface layer model for animated character construction," 1993, in Computer Graphics International'93.

[17] J. P. Lewis, M. Cordner, and N. Fong, "Pose space deformation: a unified approach to shape interpolation and skeleton-driven deformation," in *SIGGRAPH '00: Proceedings of the 27th annual conference on Computer graphics and interactive techniques*. New York, NY, USA: ACM Press/Addison-Wesley Publishing Co., 2000, pp. 165–172.

[18] P. Joshi, W. Tien, M. Desbrun, and F. Pighin, "Learning controls for blend shape based realistic facial animation," 2003, in SCA'03.

[19] W. M. Hsu, J. F. Hughes, and H. Kaufman, "Direct manipulation of free-form deformations," *SIGGRAPH Comput. Graph.*, vol. 26, no. 2, pp. 177–184, 1992.

[20] K. Singh and E. L. Fiume, "Wires: a geometric deformation technique," 1998, in SIGGRAPH'98.

[21] D. Fidaleo, J. Y. Noh, T. Kim, R. Enciso, and U. Newumann, "Classification and volume morphing for performance-driven facial animation," 2000, in Int. Workshop on Digital and Computational Video.

[22] J. X. Chai, J. Xiao, and J. Hodgins, "Visionbased control of 3d facial animation," 2003, in SCA'03.

[23] R. Falk, D. Minter, C. Vernon, G. Aretos, L. Modesto, A. Lamorlette, N. Walker, T. Cheung, J. Rentel-Lavin, and H. Max, "Art-directed technology: Anatomy of a shrek 2 sequence," 2004, ACM SIGGRAPH'04 Course Notes, ACM Press, NY, USA.

[24] J. Schleifer, "Character setup from rig mechanics to skin deformations: A practical approach," 2004, ACM SIGGRAPH'02 Course Notes, ACM Press, NY, USA.

[25] C. Maraffi, "Maya character cretion: Modeling and animation controls," 2003, new Riders Publishing.

[26] A. Ward, "Game character development with maya," 2004, new Riders Publishing.

[27] F. L. Bookstain, "Principal warps: Thin-plate splines and the decomposition of deformations," 1989, iEEE Trans. Pattern Anal. Mach. Intell. 11, 6, 567'585.

[28] J. Haber and D. Terzopoulos, "Facial modeling and animation," in *SIGGRAPH '04: ACM SIGGRAPH 2004 Course Notes*. New York, NY, USA: ACM, 2004, p. 6.

Interaction Between Virtual Characters and Humans in Rehabilitation Domain

José Carlos Miranda and Verónica Orvalho

One of the most important aspects in character animation is facial expression. The human face is crucial for the recognition and understanding of emotions. Individuals with Autism Spectrum Disorder tend to avoid looking at human faces and find it hard to recognize facial expressions and emotions in themselves and others. This incapacity to read emotions on the human face impairs their ability to communicate with other people. Our goal is to create a system to teach autistic people to recognize emotions from facial expression. The system will be able to analyze facial behavior and human emotions, and to make avatars responding to the human behavior in real-time. We will develop a classification methodology with a set of rules that specify all the facial changes that occur in facial expression. We will also develop real-time facial synthesis algorithms to display a large number of subtle expressive variations on the face. As a result of our research we will develop a facial emotion recognition system for therapeutic purposes based on our core methods. The system will consist on a game based approach that will build upon a patient-therapist relationship. It will be evaluated and validated by a group of psychology experts.

State of the Art

The facial expression is highly important in the transmission of emotions. Individuals with autism tend to avoid looking at human faces and find it hard to recognize facial expressions and emotions in themselves and others [1]. This incapacity to read emotions on the human face impairs their ability to communicate with other people [2]. Previous work has shown that children and adults with Autism Spectrum Disorders (ASD) can improve their emotion recognition skills with intervention [3, 4]. An increasing number of studies show that computer technology used in teaching and therapy is well accepted by individuals with ASD [5]. Most of these computer-based solutions aim at a teaching environment. They make use of some of the benefits afforded by computer technology, but are often based on exactly the same concepts as tried-and-true, lower-tech solutions [6]. One could argue that the rather traditional approach of these technologies fails to exploit some of the most novel and interesting properties of computer-based high technology.

> Can we extend the use of technology beyond a teaching scenario to help people with autism to look at the human face and to learn about emotions?

Facial animation has been an area of intensive research and is currently in great demand, because the human face performs an important role in verbal and non-verbal communication between humans and virtual characters. Facial expressions are generated by contractions of facial muscles, which results in temporally deformed facial features such as eye lids, eye brows, nose or lips, often revealed by wrinkles and bulges. These facial movements convey the emotional state of the individual to observers and are referred by [7] as Subtle and Micro Expressions. To recognize and classifying facial expressions it is crucial to know the facial signals that implies each facial expression. So, it is necessary to accurately describe the location of facial features, their intensity and their dynamics.

Most automatic facial expression analyses approaches [8] code facial motion and deformation into visual classes. Hence, a complete description framework would ideally contain all possible perceptible changes that may occur on a face. So, defining an optimal set of parameters that can be used to control facial movements is required. The objective is to describe the face with a small set of control parameters instead of the complete face geometry. Developing an optimal parameterization is a difficult and complex task. Research has shown that an ideal parameterization does not exist because it is difficult to satisfy all user demands for a broad range of facial applications. Parke [9] developed the first facial parametric model that allowed direct creation of facial deformation by defining ad hoc parameters or by deriving parameters from the structure and anatomy of the face. Eckman and Friesen [10] defined the Facial Action Coding Systems (FACS) to describe and measure facial behaviors. FACS became a standard when categorizing physical expressions of emotions. Animators and psychologists currently use it. The MPEG-4 Facial Anima-

tion specification was the first facial control parameterization to be standardized into MPEG-4 FBA (Face and Body Animation).

Human facial expression has been studied for more than hundred years. Computerized facial animation began in the 70's. It is interesting to understand that the techniques that are used nowadays come from the principles developed more than thirty years ago. Different approaches have been presented and developed since then and were classified into two major categories: 3D Geometric manipulation and 2D image manipulation. It is not easy to fit a certain method into one of these categories, once the boundaries between both technologies are not clearly defined. There are several approaches such as shape interpolation, geometric deformation, physically based, motion capture and re-targeting. Noh and Neumann [11] and Deng and Noh [12] presents a survey that classifies these different facial animation methods. Analysis and facial comprehension is another area that influences recent facial synthesis tendencies. Zhao et al. [13] presents a detailed document about facial recognition that gives a different perspective and complement the actual research.

Objectives

To help autistic people to recognize emotions from facial expression, we aim to create a system capable of analyzing the facial behavior and emotions of a human, and making the avatars respond to the human behavior in real-time. To analyze the facial behavior and emotions of a human we need to have a clear knowledge of the facial anatomy and sensitivity to recognize and classify a multitude of subtle expressive variations on the face, including micro expressions and subtle expressions. Also, we need to develop methods and algorithms for facial synthesis in real-time. There are several goals to achieve:

- Map facial features captured from humans to 3D avatars.
- Create a facial expression analyzer and classification method.
- Develop a real-time facial synthesis engine for different type avatars, even with distinct proportions and appearance (human, cartoon or creature).
- Develop algorithms that keep the visual appearance balance of the facial animations between photo-realistic, anatomically correct and artist look.
- Design a model interaction that involves the autistic individual more deeply in the emotions learning process.
- Define a real-time interaction methodology between human (patient or therapist) and avatars.

As a result we will be able to create different games and applications based on our core methods that will help autistic people to learn to recognize emotions, improving their ability to communicate with other people. The system will be designed to be used by a therapist and a patient and could be controlled by both, the therapist and the patient.

Acknowledgement

Joint research with Prof. Augusto de Sousa, FEUP.

Bibliography

[1] S. Baron Cohen, *Mindblindness: An essay on autism and theory of mind.* MIT Press/Bradford Books, 1995.

[2] A. P. Association, *DSM-IV diagnostic and statistical manual of mental disorders (4th Edn.).* Washington DC: American Psychiatric Association, 1994.

[3] S. Baron-Cohen, A. Spitz, and P. Cross, "Can children with autism recognize surprise?" *Cognition and Emotion*, no. 7, pp. 507–516, 1993.

[4] O. Golan, S. Baron-Cohen, E. Chapman, and Y. Granader, "Facilitating emotional understanding and face processing in young children with autism spectrum conditions, using animations of vehicles with faces," *Paper presented at the International Meeting for Autism Research (IMFAR)*, 2007.

[5] D. Moore, P. McGrath, and J. Thorpe, "Computer-aided learning for people with autism - a framework for research and development," *Innovations in Education and Training International*, no. 37, pp. 218–228, 2000.

[6] P. Michel, "The use of technology in the study, diagnosis and treatment of autism." *Final term paper for CSC350: Autism and Associated Development Disorders.*, 2004.

[7] P. Ekman, *Micro Expression Training Tool/Subtle Expression Training Tool CD*. Amazon.com, 2005.

[8] M. Pantic and L. Rothkrantz, "Automatic analysis of facial expressions: The state of the art," *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, vol. 22, no. 12, pp. 1424–1445, DEC 2000.

[9] F. Parke, "A parametric model for human faces," *Ph.D. Thesis*, 1974.

[10] P. Ekman and W. Friesen, "Facial action coding system," *Consulting Psychologist Press*, 1978.

[11] J. Noh and U. Neumann, "A survey of facial modeling and animation techniques," *USC Technical Report 99-705*, 1998.

[12] Z. Deng and J. Noh, *Computer Facial Animation: A Survey. Data-Driven 3D Facial Animation*. Springer London, 2007.

[13] W. Zhao, R. Chellappa, P. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM COMPUTING SURVEYS*, vol. 35, no. 4, pp. 399–459, DEC 2003.

T-LIFE: Therapeutic LearnIng of Facial Emotions

Verónica Orvalho and Miguel Coimbra

The face is the key element to convey emotion and plays an important role in verbal and non-verbal communication. Many efforts have been done to teach people with Autism Spectrum Disorders (ASD) to recognize facial expressions with varying results [1], but none focused on using real time facial synthesis. Most methodologies use Paul Ekman's approach [2] based on photographs of facial expressions. Besides having severely limited interactivity, they fail to reproduce the dynamics of a facial expression: far from being a still image, it is the voluntary and involuntary contraction of muscles that produce different facial movements. These movements convey emotions from one individual to another, enabling non-verbal communication. Thus, we need to weigh in an additional teaching method that allows facial motion. Then, it is necessary to study techniques that will allow real-time facial synthesis. T-LIFE is designed to assist people with ASD to recognize facial expressions in a playful way. The key technological contributions of this project are: a real-time facial markerless motion capture system, a new facial expression analyzer and classification method and an immersive interaction model.

T-LIFE aims to improve the ability of socially and emotionally impaired individuals to recognize and respond to emotions conveyed by the face by means of Therapeutic Learning Tools.

Introduction

T-LIFE aims to improve the ability of socially and emotionally impaired individuals to recognize and respond to emotions conveyed by the face by means of Therapeutic Learning Tools.

We argue that current technological advances in character animation can substantially improve the way we teach people with Autism Spectrum Disorders (ASD) to recognize facial expressions. Our approach introduces a novel and sophisticated interaction model that enables patients to learn by imitating the avatars movements. Our work includes a thorough field test with therapists and patients to validate our methodology, which will be performed by APPDA, FPCE/UP and Stanford University School of Medicine.

A substantial part of our research is targeted towards 3D avatars capable of teaching individuals with social phobia, anxiety and ASD, how to improve personal interactions. The main outcome will be a comprehensive system that analyzes the facial behavior of a human and enables avatars to respond to it in real-time. The avatars are 3D models with underlying anatomical behavior, and have a wide range of visual styles: human, cartoon or fantasy creature. We shall develop a prototype, which will run on PCs and game consoles, that builds upon the patient-therapist relationship: it is designed to be used both by the therapist and the patient, but also by parents and teachers. The prototype will include a set of exercises to help the patient improve his interactions with other people.

In previous work where people interact with a virtual character, the virtual character representations have been quite simple, and little or no attention was paid to facial expression [3]. Here we intend to incorporate the full range of facial expressions based on a geometric and muscle model, thus giving a much greater repertoire of possible expressions. Moreover, in the context of our solution, it is possible to feedback the patients' own facial expression as captured on a webcam, by mapping it into a virtual character and allowing them to see a representation of themselves in a virtual mirror. As they look into this mirror and change their own facial expressions, they will see their virtual mirror image change accordingly. This can, with the help of the trainer, be used as part of a feedback loop, so that the patient can learn to control facial expressions in a playful way, without induction of stress. For example, suppose that the patient looks in the mirror and sees himself as a famous cartoon character which nevertheless reflects their own facial movements; this is something to be enjoyed rather than a difficult process of learning.

The technology behind the prototype is based on the facial synthesis of 3D characters. The main research challenges arise from

the synchronization and realism problems, the support for the reusability of facial components, and the need for an avatar-user interaction model with real time response. Traditional techniques to achieve high quality facial animation include keyframe animation and motion capture based on facial markers. These solutions are not suitable for our approach, because keyframe animation is very laborious and time-consuming and motion capture requires the user to wear markers in the face, which is unpleasant and " unnatural" . To overcome these problems, we will develop a markerless facial motion capture system that uses low cost hardware, like a webcam, to capture the information, and create a sophisticated facial rig capable of reproducing the subtleties of a face through animation. A rig is a set of controls that allows animating a character. This is not a trivial task, as we are using low resolution input data to drive the face model animations. Thus, this rig becomes the foundation of the system pipeline. It will ensure that the characters animations follow a consistent artistic style, to ease the process of recognizing facial expressions and emotions. The PI has successfully demonstrated in her SIGGRAPH07 work [4] that re-targeting of facial rigs is possible and it is key to obtain high quality animations. As far as we know, there is no facial markerless motion capture system that runs in real-time and produces cinematographic quality results.

The Team

To carry out this project and achieve its goals, we have gathered an interdisciplinary team, as well as external consultants, which include experts in the study of presence in virtual environments (Dr. Slater), in facial character animation (Dra. Orvalho), in speech synthesis and recognition (Dr. Sales Dias), in rendering and computational photography (Dr. Gutierrez), in human-computer interaction (Dr. Julián Flores), in pattern recognition and computer vision (Dr. Coimbra) and in Autism Spectrum Disorder (Dr. Fienstein, Dra. Freitas and Dra. Queirós). We expect to include in the near future experts from Germany, Switzerland and the UK on geometric modeling and deformation, game design and global illumination effects for interactive applications. Our current industrial partner is Microsoft.

Research Problems

We shall address the following research problems: **1.** Develop a markerless facial motion capture system that uses low cost hardware, like a webcam, and is still capable of reproducing in real-time cinematographic quality facial animations. As far as we are aware, this type of system doesn't exist. **2.** Create a facial expression analyzer and classifier system that provides facial detail information that cannot be captured using current motion capture systems. We will explore novel computer graphics algorithms. **3.** Explore different user interaction models to define them most adequate tangible user interface to allow an immersive behavior when interacting with people that suffer of ASD. Current approaches lack of an efficient HCI methodology. **4.** Study and propose a novel interactive learning environment that will improve social and communication skills by training interpersonal awareness through facial recognition. **5.** Deploy a prototype that enhances the ability to observe and recognize emotions through an interactive experience and becomes a key reference in this field.

Conclusion

There are four important potential repercussions of the T-LIFE project: technological, scientific, clinical and social.

Technological: We aim to become a key reference in the field of facial animation in real-time, as our technology can speed up the character animation process by capturing a performer facial movements directly to multiple 3D models. It will enable creating animations on the fly by scripting facial behaviors, using our facial expression analyzer and classifier system. Then, non-experienced users will be able to create high quality animations. Having a person simply tell the system how an expression is, by describing it in a high level language is immensely empowering.

Scientific: We aim to set the foundation of a new generation of facial synthesis algorithms by exploring the emerging domain of markerless facial motion capture, and the research of novel solutions on the field of facial expression recognition.

Clinical: We will develop a prototype that can be used for validating this new approach for helping autistic people in identifying and expressing emotions. The novelty of this approach is the interactivity of the process, as opposed to previous methods using still images.

Societal: Integration of socially impaired people, which will help them become a contributing member of a advanced society.

Bibliography

[1] O. G. et al., "Facilitating emotional understanding and face processing in young children with asd, using animations of vehicles with faces. 2007."

[2] P. Ekman and W. Friesen, "Unmasking the face. 1975."

[3] X. Pan and M.Slater, "A preliminary study of shy males interacting with a virtual female," *In PRESENCE 2007*.

[4] V. Orvalho, "Reusable facial rigging and animation," Ph.D. dissertation, UPC, 2007.

Real-time muscle system for automatic placement and animation, with collision detections

Verónica Orvalho and Bruno Oliveira

Face muscles play a very important role in the capability to express emotions, and whence a significant effort is made everyday by users, both professional and non-professional, to place and animate muscles. The capacity to express emotions is achieved by the movement of the muscles beneath the skin, that make the face contract or expand, and produce expression marks, like wrinkles, that occur when the skin collides with itself.

The placement and animation of muscles is, nowadays, a manual process, that is both tedious and time consuming. Users tweak every muscle in order to achieve the desired animation, and, in many cases, the collision detection between the several elements prevents the task from being real-time.

We present a new real-time automatic approach that could ease the process, drastically reducing the required time for the task and skill levels, and capable of dealing with the intense collisions that occurs while muscles move. Some developments have already been made in the area of automatic muscle placement [1], but the results still present some problems.

Introduction

In computer graphics terms, muscles are modeled as deformable soft bodies placed underneath the set of points representing the skin, called mesh, and, possibly, under other deformable soft bodies representing fat tissue. When these muscles change shape, they collide with the fat tissue and the skin, producing movement. This Ph.D. proposal will try to address three problems that are disclosed above: the placement of the deformable objects representing the muscles, the collision between these muscles and the fat tissue and skin — furthermore, the movement of the fat tissue and the skin, produces even more collision between them —, and the automatic animation of the muscles that provide the subtle deformations on the face.

In order to create and place the muscles, the common practice is that users model specific modifiers underneath the mesh — deformable soft bodies that act on the surroundings —, indicating origin and insertion points, and then a tweak and adjust phase follows, where users define the properties of each muscle, like shape, stretch volume, sliding, or the weight of it to the movement of the mesh, achieving the desired movement.

This represents a very meticulous and time consuming task, which requires a highly skilled user, with some anatomy knowledge. We expect to contribute with a more intuitive approach, that can render the task of muscle creation and placement much quicker and easier, using natural interfaces, usability and operational research.

Workflow

The proposed workflow goes as follows: first, the user draws the muscles in a representation of the mesh. Then, using this information, the system infers the correct position, shape, and most properties of the muscle automatically. Finally, necessary adjustments can be performed in a context aware interface, that minimizes the cluttering that can occur when a high level of variables are in play. With this approach we believe that the task of placement and animation of facial muscles can be reduced from days to a some hours.

Although this may seem a simple workflow, and that is the main idea from the point of view of the user, the system will have to deal with a problem with a high level of complexity, in computer sciences terms, that is the inference of the muscles based on the input.

Some research has already been done in this field [2], but an optimal result is yet to be obtained, and will pass by the development of advanced heuristics, since this is not a trivial problem.

This research will be supported by the work of my advisor, Prof. Verónica Orvalho, that developed a system to reuse facial rigging and animation [3].

Real-time collisions detection

As a complement to this research, since the automatic placement of the muscles and consequent animation in real-time will have to deal with the collisions between these and the skin and fat tis-

sue, we expect to research a real-time solver for deformable soft bodies collisions for facial muscles.

Deformable soft bodies require a much higher level of collision detections than rigid bodies, because they change shape, maintaining volume, as the collisions occur. This renders an exponential number of calculations, but some research [4] is already showing very interesting results regarding a real-time performance.

Application and contributions

The main areas of application of the thesis results are the entertainment industry, the movies industry. However, it can also be applied to projects that require quick, but correct, muscle placement and animation, such as T-Life [5], that is designed to assist people with Autism Spectrum Disorders to recognize facial expressions.

Main contributions of the Ph.D. thesis: easy and intuitive muscle placement and animation system for faces, human or not, to drastically reduce the work and the time required by users in this task, and a real-time muscle-to-skin and skin-to-skin interaction system, that will profoundly increase the level of the perceived realism in the face expressions.

Bibliography

[1] E. Sifakis, I. Neverov, and R. Fedkiw, "Automatic determination of facial muscle activations from sparse motion capture marker data," *ACM Trans. Graph.*, vol. 24, no. 3, pp. 417–425, July 2005. [Online]. Available: http://dx.doi.org/10.1145/1073204.1073208

[2] K. Kohler, J. Haber, and H. peter Seidel, "Geometry-based muscle modeling for facial animation," in *In Proc. Graphics Interface 2001*, 2001, pp. 37–46.

[3] V. C. Orvalho and A. Susin, "Fast and reusable facial rigging and animation," in *SIGGRAPH '07: ACM SIGGRAPH 2007 sketches*. New York, NY, USA: ACM, 2007, p. 63.

[4] G. Irving, C. Schroeder, and R. Fedkiw, "Volume conserving finite element simulations of deformable models," in *SIGGRAPH '07: ACM SIGGRAPH 2007 papers*. New York, NY, USA: ACM, 2007, p. 13.

[5] V. C. Orvalho, M. T. Coimbra, M. D. Dias, M. Slater, D. Gutierrez, and J. Flores, "T-life: Therapeutic learning of facial emotions," 2009.

instituto de telecomunicações

Publications

Books or Book Chapters in 2007

[1] J. Barros, *Sensor Networks: An Overview*, ser. In Learning from Data Streams - Processing Techniques in Sensor Networks. Springer Verlag, 2007.

Journal Papers in 2007

[1] J. Barros and M. Tuechler, "Estimation of functionals over noisy channels," *European Transactions on Telecommunications*, vol. Vol.18, no. No.8, 2007.

[2] I. A. Chatzigeorgiou, M. R. D. Rodrigues, I. J. Wassell, and R. A. Carrasco, "A comparison of convolutional and turbo coding schemes for broadband fwa systems," *IEEE Transactions on Broadcasting*, vol. 53, pp. 494–503, June 2007.

[3] J. A. Adeane, M. R. D. Rodrigues, and I. J. Wassell, "Lattice reduction based detection techniques for mimo-ofdm-cdm communication systems," *IET Communications*, vol. 1, pp. 526–531, June 2007.

[4] ——, "Centralised and distributed power allocation for cooperative networks," *Electronics Letters*, vol. 43, pp. 39–40, January 2007.

[5] M. Coimbra, M. Mackiewicz, M. Fisher, C. Jamieson, J.Soares, and J. S. Cunha, "Computer vision tools for capsule endoscopy exam analysis," *invited paper in Eurasip NewsLetter*, vol. 18/1, pp. 1–19, March 2007.

[6] M. C. Domingo and R. Prior, "An adaptive gateway discovery algorithm to support qos when providing internet access to mobile ad hoc networks," *Journal of Networks*, vol. 2, no. 2, pp. 33–44, 2007.

[7] R. Prior and S. Sargento, "Cross-layer mobility with sip and mipv6," *Journal of Internet Technology*, vol. 8, no. 3, 2007.

[8] ——, "Inter-domain qos routing - optimal and practical study," *IEICE Transactions on Communications*, vol. E90-B, no. 3, pp. 549–558, 2007.

[9] ——, "Scalable reservation-based qos architecture - srbq," *Encyclopedia of Internet Technologies and Applications*, pp. 473–482, 2007.

Conference Papers in 2007

[1] P. F. Oliveira and J. Barros, "Network coding protocols for secret key distribution," in *Proceedings of the International Symposium on Information Security (IS'07)*, Vilamoura, Portugal, November 2007.

[2] M. Bloch, J. Barros, and S. W. McLaughlin, "Practical information-theoretic commitment," in *Proceedings of the Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, USA, September 2007.

[3] J. Barros, "Codes for sensors: An algorithmic perspective," in *Proceedings of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS'07)*, Wroclaw, Poland, July 2007.

[4] L. B. Lopes, F. Martins, M. S. Silva, and J. Barros, "A process calculus approach to sensor networks," in *Proceedings of the International Conference on Sensor Technologies and Applications (SENSORCOMM'07)*, Valencia, Spain, October 2007.

[5] G. Maierbacher and J. Barros, "Diophantine index assignments for distributed source coding," in *Proceedings of the IEEE Information Theory Workshop (ITW'07)*, Lake Tahoe, California, USA, September 2007.

[6] J. P. Vilela and J. Barros, "A feedback reputation mechanism to secure the optimized link state routing protocol," in *Proceedings of the IEEE Communications Society/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm'07)*, Nice, France, September 2007.

[7] P. F. Oliveira, R. A. Costa, , and J. Barros, "Mobile secret key distribution with network coding," in *Proceedings of the International Conference on Security and Cryptography (SECRYPT'07)*, Barcelona, Spain, July 2007.

[8] L. Lopes, F. Martins, M. S. Silva, , and J. Barros, "Formal model for programming wireless sensor networks," in *Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS'07)*, Santa Fe, New Mexico, USA, June 2007.

[9] M. M. L. Lima and J. Barros, "Random linear network coding: A free cypher?" in *Proceedings of the IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[10] R. A. Costa and J. Barros, "Dual radio networks: Capacity and connectivity," in *Proceedings of the Workshop on Spatial Stochastic Models in Wireless Networks (SpaSWiN'07)*, Limassol, Cyprus, April 2007.

[11] L. Lima and J. Barros, "Random walks on sensor networks," in *Proceedings of the 5th International Syposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt'07),*, Limassol, Cyprus, April 2007.

[12] G. Maierbacher and J. Barros, "Code design for the distributed scalar quantization problem based on diophantine analysis," in *Proceedings of the IEEE Information Theory Winter School*, La Colle sur Loup, France, March 2007.

[13] J. Barros and M. Tuechler, "Decoding a function from noisy sensor data: A factor graph approach," in *Proceedings of the 41st Annual Conference on Information Sciences and Systems (CISS'07)*, Baltimore, Maryland, USA, March 2007.

[14] J. N. Laneman and J. Barros, "Rate-equivocation tradeoffs," in *Proceedings of the Information Theory and Applications Workshop*, San Diego, USA, February 2007.

[15] M. Bloch, J. Barros, M. R. D. Rodrigues, , and S. W. McLaughlin, "Information-theoretic security for wireless channels: Theory and practice," in *Proceedings of the Information Theory and Applications Workshop*, San Diego, USA, February 2007.

[16] F. Perez-Cruz, M. R. D. Rodrigues, and S. Verdu, "Generalized mercury/waterfilling for multiple-input multiple-output channels," in *Proceedings of the 45th Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, USA, September 2007.

[17] J. M. B. Oliveira, M. R. D. Rodrigues, and H. M. Salgado, "Optimum receivers for non-linear distortion compensation of OFDM signals in fiber supported wireless applications," in *Proceedings of the 2007 IEEE International Topical Meeting on Microwave Photonics*, Victoria, British Columbia, Canada, October 2007.

[18] W. R. Carson, I. A. Chatzigeorgiou, I. J. Wassell, M. R. D. Rodrigues, and R. A. Carrasco., "On the performance of iterative demapping and decoding over quasi-static fading channels," in *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Athens, Greece, September 2007.

[19] J. M. B. Oliveira, M. R. D. Rodrigues, and H. M. Salgado, "Non-linear distortion compensation of OFDM signals in radio-over-fiber systems," in *Proceedings of the V Symposium on Enabling Optical Networks and Sensors*, Aveiro, Portugal, June 2007.

[20] I. A. Chatzigeorgiou, M. R. D. Rodrigues, I. J. Wassell, and R. A. Carrasco, "Pseudo-random puncturing: A technique to lower the error floor of turbo codes," in *Proceedings of the IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[21] J. A. Adeane, M. R. D. Rodrigues, and I. J. Wassell, "Partner selection schemes for cooperative networks," in *Proceedings of the Signal Processing for Wireless Communications Workshop*, London, U.K., June 2007.

[22] I. A. Chatzigeorgiou, M. R. D. Rodrigues, I. J. Wassell, and R. A. Carrasco, "A union bound approximation for rapid performance evaluation of punctured turbo codes," in *Proceedings of the 41st Annual Conference on Information Sciences and Systems*, Baltimore, Maryland, USA., March 2007.

[23] S. Bessa, E. Correia, and P. Brandao, "Storage and retrieval on P2P networks: A DHT based protocol," in *Proceedings of the 12th IEEE Symposium on Computers and Communications (ISCC'07)*, Aveiro, Portugal, July 2007.

[24] M. C. Domingo and R. Prior, "Design and analysis of a GPS-free routing protocol for underwater wireless sensor networks in deep water," in *Proceedings of the International Conference on Sensor Technologies and Applications (SENSORCOMM'07)*, Valencia, Spain, October 2007.

[25] ——, "A distributed clustering scheme for underwater wireless sensor networks," in *Proceedings of the 18th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)*, Athens, Greece, September 2007.

[26] R. Prior and S. Sargento, "Inter-domain QoS routing with virtual trunks." in *Proceedings of the IEEE International Conference on Communications (ICC'07)*, Glasgow, Scotland, June 2007.

[27] ——, "SIP and MIPv6: Cross-layer mobility," in *Proceedings of the 12th IEEE Symposium on Computers and Communications (ISCC'07)*, Aveiro, Portugal, July 2007.

Books or Book Chapters in 2008

[1] J. Barros, *Information Flows in Complex Networks*, ser. In Information Theory and Statistical Learning. Springer Verlag.

Journal Papers in 2008

[1] A. Nascimento, J. Barros, S. Skudlarek, and H. Imai, "The commitment capacity of the gaussian channel is infinite," *IEEE Transactions on Information Theory, Special Issue on Information-Theoretic Security*, vol. Vol.54, no. No. 6, pp. 2785–2789, 2008.

[2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory, Special Issue on Information-Theoretic Security*, vol. Vol. 54, no. No. 6, pp. 2515–2534, 2008.

[3] P. F. Oliveira and J. Barros, "A network coding approach to secret key distribution," *IEEE Transactions on Information Forensics and Security*, vol. Vol. 3, no. No. 3, pp. 414–423, 2008.

[4] G. Maierbacher and J. Barros, "Source-optimized clustering and distributed quantization for large-scale sensor networks," *ACM Transactions on Sensor Networks*, 2008.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory - Special Issue on Information-Theoretic Security*, vol. vol. 54, pp. 2515–2534, 2008.

[6] J. S. Cunha, M. Coimbra, P. Campos, and J. Soares, "Automated topographic segmentation and transit time estimation in endoscopic capsule exams," *IEEE Transactions in Medical Imaging*, 2008.

[7] M. C. Domingo and R. Prior, "Energy analysis of routing protocols for underwater wireless sensor networks," *Computer Communications*, 2008.

Conference Papers in 2008

[1] S. Crisóstomo, J. Barros, and C. Bettstetter, "Network coding with shortcuts," in *Proceedings of the IEEE International Conference on Communication Systems*, Guangzhou, China, November 2008.

[2] P. Pinto, J. Barros, and M. Win, "Physical-layer security in stochastic wireless networks," in *Proceedings of the IEEE International Conference on Communication Systems*, Guangzhou, China, November 2008.

[3] M. Kim, M. Medard, and J. Barros, "Counteracting byzantine adversaries with network coding: An overhead analysis," in *Proceedings of the IEEE Military Communications Conference*, San Diego, California, USA, November 2008.

[4] L. Lima, J. P. Vilela, J. Barros, and M. Medard, "An information-theoretic cryptanalysis of network coding - is protecting the code enough?" in *Proceedings of the International Symposium on Information Theory and its Applications*, Auckland, New Zealand, December 2008.

[5] R. A. Costa, D. Munaretto, J. Widmer, and J. Barros, "Informed network coding for minimum decoding delay," in *Proceedings of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS '08)*, Atlanta, Georgia, September/October 2008.

[6] J. Barros, "Mixing packets: Pros and cons of network coding," in *Proceedings of the 11th International Symposium on Wireless Personal Multimedia Communications*, Lapland, Finland, September 2008.

[7] J. Barros and M. Bloch, "Strong secrecy for wireless channels." in *Proceedings of the International Conference on Information-Theoretic Security*, Calgary, Canada, August 2008.

[8] A. Zuquete and J. Barros, "Physical-layer encryption using stream ciphers," in *Proceedings of the IEEE International Symposium on Information Theory*, Toronto, Ontario, Canada, July 2008.

[9] H. C. ao, M. Ferreira, and J. Barros, "On the urban connectivity of vehicular sensor networks," in *Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '08)*, Santorini Island, Greece, June 2008.

[10] S. Crisóstomo, J. Barros, and C. Bettstetter, "Flooding the network: Multipoint relays versus network coding," in *Proceedings of the IEEE International Conference on Circuits and Systems for Communications*, Shanghai, China, May 2008.

[11] J. P. Vilela, L. Lima, and J. Barros, "Lightweight security for network coding," in *Proceedings of the IEEE International Conference on Communications (ICC2008)*, Beijing, China, May 2008.

[12] H. C. ao, L. Damas, M. Ferreira, and J. Barros, "Large-scale simulation of v2v environments," in *Proceedings of the ACM 2008 Symposium on Applied Computing (SAC'08)*, Fortaleza, Brazil, March 2008.

[13] M. R. D. Rodrigues and P. D. M. Almeida, "Filter design with secrecy constraints: The degraded parallel gaussian wiretap channel," in *Proceedings of the IEEE Global Communications Conference*, New Orleans, Louisiana, USA, December 2008.

[14] J. M. B. Oliveira, M. R. D. Rodrigues, and H. M. Salgado, "Optimum receivers for non-linearly distorted OFDM signals in wireless-over-fiber applications: Impact of antenna noise," in *Proceedings of the IEEE International Conference on Ultra-Wideband*, Hannover, Germany, September 2008.

[15] I. Kanaras, A. Chorti, M. R. D. Rodrigues, and I. Darwazeh, "Optimum detection for a spectrally efficient non-orthogonal FDM system," in *Proceedings of the 13th International OFDM-Workshop*, Hamburg, Germany, September 2008.

[16] ——, "A combined MMSE-ML detection scheme for a spectrally efficient non-orthogonal FDM signal," in *Proceedings of the Fifth International Conference on Broadband Communications, Networks, and Systems*, London, U.K., September 2008.

[17] W. R. Carson, M. R. D. Rodrigues, and I. J. Wassell, "Optimal 8PSK mappings for BICM-ID over quasi-static fading channels," in *Proceedings of the 5th International Symposium on Turbo Codes and Related Topics*, Lausanne, Switzeerland, September 2008.

[18] F. Perez-Cruz, M. R. D. Rodrigues, and S. Verdu, "Optimal precoding for digital subscriber lines," in *Proceedings of the IEEE International Conference on Communications*, Beijing, China, May 2008.

[19] M. R. D. Rodrigues, F. Perez-Cruz, and S. Verdu, "Multiple-input multiple-output gaussian channels: Optimal covariance for non-gaussian inputs," in *Proceedings of the IEEE Information Theory Workshop*, Porto, Portugal, May 2008.

[20] I. Kanaras, A. Chorti, M. R. D. Rodrigues, and I. Darwazeh, "Sub-optimum detection techniques for a bandwidth efficient multi-carrier communication system," in *Proceedings of the Cranfield Multi-Strand Conference*, Cranfield University, Milton, U.K., May 2008.

[21] W. R. Carson, M. R. D. Rodrigues, and I. J. Wassell, "Modelling the framer error rate for iterative demapping and decoding over quasi-static fading channels," in *Proceedings of the IEEE Sarnoff Symposium*, Princeton, New Jersey, USA, April 2008.

[22] A. Sousa, M. Dinis-Ribeiro, M. Areia, M. Correia, and M. Coimbra, "Towards more adequate colour histograms for in-body images," in *Proceedings of the IEEE Engineering in Medicine and Biology Conference (EMBC'08)*, Vancouver, British Columbia, Canada, August 2008.

Books or Book Chapters in 2009

[1] P. Xiao, I. A. Chatzigeorgiou, M. R. D. Rodrigues, I. J. Wassell, and R. A. Carrasco, *Design Considerations and Algorithms for Broadband Fixed WiMAX Systems*, ser. VLSI and Computer Architecture. Nova Science Publishers, 2009.

[2] A. Ferreira, L. Barreto, P. Brandao, R. Correia, S. Sargento, and L. Antunes, *Accessing an existing virtual electronic patient record with a secure wireless architecture*, ser. Mobile Health Solutions for Biomedical Applications. IGI Global, 2009.

Journal Papers in 2009

[1] G. Maierbacher and J. Barros, "Source-optimized clustering and distributed quantization for large-scale sensor networks," *ACM Transactions on Sensor Networks*, vol. 5, no. 3, May 2009.

[2] M. Boban, O. Tonguz, and J. Barros, "Unicast communication over vanet: A reality check," *IEEE Communications Letters*, 2009, to appear.

[3] L. Lima, F. Zhao, J. Barros, M. Medard, R. Koetter, T. Kalker, and K. Han, "On counteracting byzantine attacks in network coded peer-to-peer networks," *IEEE Journal of Selected Areas in Communications*, 2009, to appear.

[4] I. A. Chatzigeorgiou, A. Demosthenous, M. R. D. Rodrigues, and I. J. Wassell, "On the performance-complexity tradeoff of convolutional codes for broadband fwa systems." *IET Communications*, 2009, to appear.

[5] F. Pérez-Cruz, M. R. D. Rodrigues, and S. Verdú, "Mimo gaussian channels with arbitrary inputs: Optimal precoding and power allocation," *IEEE Transactions on Information Theory*, 2009, to appear.

[6] I. A. Chatzigeorgiou, M. R. D. Rodrigues, I. J. Wassell, and R. A. Carrasco, "Analysis and design of punctured rate-1/2 turbo codes exhibiting low error floors," *IEEE Journal on Selected Areas in Communications - Special Issue on Capacity Approaching Codes*, vol. 27, pp. 944–953, August 2009.

[7] ——, "The augmented state diagram and its applications to convolutional and turbo codes," *IEEE Transactions on Communications*, vol. 57, pp. 1948–1958, July 2009.

[8] P. Ribeiro, H. Simões, and M. Ferreira, "Teaching artificial intelligence and logic programming in a competitive environment," *Informatics in Education*, vol. 8, no. 1, pp. 85–100, 2009.

Conference Papers in 2009

[1] J. Almeida and J. Barros, "Joint compression and data protection," in *Proceedings of the Forty-Seventh Annual Allerton Conference on Communication, Control and Computing*, Monticello, Illinois, USA, September/October 2009.

[2] D. Klinc, J. Ha, S. W. Mclaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for physical layer security," in *Proceedings of the IEEE Globecom 2009 (Communications and Information Security Symposium)*, Honolulu, Hawaii, USA, November/December 2009.

[3] ——, "LDPC codes for the gaussian wiretap channel," in *Proceedings of the IEEE Information Theory Workshop*, Taormina, Italy, October 2009.

[4] L. Lima, J. Barros, M. Medard, and A. Toledo, "Protecting the code: Secure multiresolution network coding," in *Proceedings of the IEEE Information Theory Workshop*, Volos, Greece, June 2009.

[5] R. Meireles, M. Ferreira, and J. Barros, "Vehicular connectivity models: From single-hop links to large-scale behavior," in *Proceedings of the IEEE Vehicular Technology Conference: VTC2009-Fall*, Anchorage, Alaska, USA, September 2009.

[6] D. Ferreira, L. Lima, and J. Barros, "Network coding protocols: Does topology matter?" in *Proceedings of the Future Internet Architectures Workshop: New Trends in Service Architectures (2nd Euro-NF Workshop)*, Santander, Spain, June 2009.

[7] J. B. G. Maierbacher and M. Medard, "Practical source-network decoding," in *Proceedings of the IEEE International Symposium on Wireless Communication Systems (ISWCS'09)*, Siena, Italy, September 2009.

[8] F. Vieira and J. Barros, "Network coding multicast in satellite networks," in *Proceedings of the 5th Euro-NGI Conference on Next Generation Internet Networks*, Aveiro, Portugal, July 2009.

[9] P. Pinto, J. Barros, and M. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proceedings of the IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009.

[10] M. Kim, M. Medard, J. Barros, and R. Koetter, "An algebraic watchdog for wireless network coding," in *Proceedings of the IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009.

[11] L. Lima, J. Barros, and R. Koetter, "Byzantine attacks against network coding in peer to peer distributed storage," in *Proceedings of the IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009.

[12] F. Vieira and J. Barros, "Network coding multicast framework for broadband satellite systems," in *Proceedings of the 7th Conference on Telecommunications*, Santa Maria da Feira, Portugal, May 2009.

[13] F. Martins, L. B. Lopes, and J. Barros, "Towards the safe programming of wireless sensor networks," in *Proceedings of the Programming Language Approaches to Concurrency and Communication-cEntric Software*, York, UK, March 2009.

[14] J. Almeida, G. Maierbacher, and J. Barros, "Low-complexity index assignments for secure quantization," in *Proceedings of the 43rd Annual Conference on Information Sciences and Systems (CISS'09)*, Baltimore, Maryland, USA, March 2009.

[15] D. Ferreira, L. Lima, and J. Barros, "NECO: Network coding simulator," in *Proceedings of the International Conference on Simulation Tools and Techniques (Simutools '09)*, Rome, Italy, March 2009.

[16] H. Conceição, M. Ferreira, and J. Barros, "Cautionary view of mobility and connectivity modeling in vehicular ad-hoc networks," in *Proceedings of the IEEE Vehicular Technology Conference (VTC2009-Spring)*, Barcelona, Spain, April 2009.

[17] J. Barros, R. A. Costa, D. Munaretto, and J. Widmer, "Effective delay control for online network coding," in *Proceedings of the IEEE Infocom 2009*, Rio de Janeiro, Brazil, April 2009.

[18] J. K. Sundararajan, D. Shah, M. Medard, M. Mitzenmacher, and J. Barros, "Network coding meets TCP," in *Proceedings of the IEEE Infocom 2009*, Rio de Janeiro, Brazil, April 2009.

[19] S. Crisóstomo, U. Schilcher, J. Barros, and C. Bettstetter, "Analysis of probabilistic flooding: How do we choose the right coin?" in *Proceedings of the IEEE International Conference on Communications (ICC'09)*, Dresden, Germany, June 2009.

[20] I. Kanaras, A. Chorti, M. R. D. Rodrigues, and I. Darwazeh, "A new quasi-optimal detection algorithm for a non orthogonal spectrally efficient FDM," in *Proceedings of the IEEE International Symposium on Communication and Information Technology*, Incheon, Korea, September 2009.

[21] ——, "Investigation of a semidefinite programming detection for a spectrally efficient FDM system," in *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Tokyo, Japan, September 2009.

[22] P. Aguiar and M. R. D. Rodrigues, "Neuronal connectivity inference from spike trains using an empirical probabilistic causality measure," in *Proceedings of the Eighteenth Annual Computational Neuroscience Meeting*, Berlin, Germany, July 2009.

[23] M. R. D. Rodrigues and G. Ramos, "On multiple-input multiple-output gaussian channels subject to jamming," in *Proceedings of the IEEE International Symposium on Information Theory*, Seoul, South Korea, June-July 2009.

[24] I. Kanaras, A. Chorti, M. R. D. Rodrigues, and I. Darwazeh, "Spectrally efficient FDM signals: Bandwidth gain at the expense of receiver complexity," in *Proceedings of the IEEE International Conference on Communications*, Dresden, Germany, June 2009.

[25] J. M. B. Oliveira, M. R. D. Rodrigues, and H. M. Salgado, "MMSE receivers for non-linearly distorted OFDM signals," in *Proceedings of the 7th Conference on Telecommunications*, Santa Maria da Feira, Portugal, May 2009.

[26] A. Sousa, M. Dinis-Ribeiro, M. Areia, and M. Coimbra, "Identifying cancer regions in vital-stained magnification endoscopy images using adapted color histograms," in *Proceedings of the IEEE ICIP 2009*, Cairo, Egypt, November 2009.

[27] F. Riaz, M. Dinis-Ribeiro, and M. Coimbra, "Quantitative comparison of segmentation methods for in-body images," in *Proceedings of the IEEE EMBC 2009*, Minneapolis, USA, September 2009.

[28] S. Lima, J. S. Cunha, M. Coimbra, and J. Soares, "ECCA – endoscopic capsule capview cataloguer," in *Proceedings of the 11th World Congress on Medical Physics and Biomedical Engineering*, Munich, Germany, September 2009.

[29] F. Riaz, A. Sousa, P. Pimentel-Nunes, M. Areia, M. Coimbra, and M. Dinis-Ribeiro, "Análise assistida por computador de imagens de cromendoscopia gástrica: praticabilidade e aplicabilidade," in *Proceedings of the 29th National Meeting in GastroEnterology*, Porto, Portugal, 2009.

[30] F. Riaz, M. Dinis-Ribeiro, and M. Coimbra, "A review of current computer aided diagnosis systems for polyp detection in virtual colonoscopy," in *Proceedings of the 7th Conference on Telecommunications*, Santa Maria da Feira, Portugal, May 2009.

[31] ——, "Semantic relevance of current image segmentation algorithms," in *Proceedings of the IEEE WIAMIS 2009*, London, UK, May 2009.

[32] S. Lima, M. Coimbra, J. Soares, and J. S. Cunha, "A tool for endoscopic capsule dataset preparation for clinical video event detector algorithms," in *Proceedings of the Healthinf 2009*, Porto, Portugal, 2009.

[33] F. Hedayioglu, S. Mattos, and M. Coimbra, "A survey of audio processing algorithms for digital stethoscopes," in *Proceedings of the HealthInf 2009*, Porto, Portugal, 2009.

[34] M. Ferreira, H. Conceição, R. Fernandes, and R. Reis, "Locating Cars through a Vision-Enabled VANET," in *Proceedings of the 2009 IEEE Intelligent Vehicles Symposium IV'09*, Xi'An, China, June 2009.

[35] D. Vaz, V. S. Costa, and M. Ferreira, "User Defined Indexing," in *Proceedings of the 25th International Conference on Logic Programming (ICLP'09)*, ser. LNCS, P. Hill and D. S. Warren, Eds. Pasadena, California, USA: Springer-Verlag, July 2009.

[36] F. Lima and M. Ferreira, "Mining Spatial Data from GPS Traces for Automatic Road Network Extraction," in *Proceedings of the 6th International Symposium on Mobile Mapping Technology (MMT'09)*, S. Paulo, Brazil, July 2009.

[37] H. Conceicao, M. Ferreira, and J. Barros, "Cautionary view of mobility and connectivity modeling in vehicular ad-hoc networks," in *Proceedings of the IEEE Vehicular Technology Conference (VTC2009-Spring)*, 2009.

[38] V. C. Orvalho, J. Miranda, and A. A. Sousa, "What a feeling: Learning facial expressions and emotions," in *Proceedings of the Videojogos Conference*, Aveiro, Portugal, November 2009.

[39] ——, "Facial sinthesys of 3d avatars for therapeutic applications," in *Proceedings of the 14th Annual CyberTherapy and CyberPsychology Conference*, Verbania-Intra, Italy, June 2009.

[40] V. C. Orvalho, M. T. Coimbra, M. S. Dias, M. Slater, D. Gutierrez, and J. Flores, "T-life: Therapeutic learning of facial emotions," in *Proceedings of the The European Future Technologies Conference*, Prague, Czech Republic, April 2009.

[41] P. Brandao and J. Bacon, "Bsn middleware: Abstracting resources to human models," in *Proceedings of the HealthInf, International Conference on Health Informatics*, 2009.

Achievements

1 Concluded M.Sc. theses

- **Fábio Hedayioglu**, DigiScope - DIGItally enhanced stethoSCOPE for clinical usage. (Supervisor: Miguel Coimbra. Concluded: 11/2009.)
- **Diogo Ferreira**, A Performance Evaluation of Network Coding. (Supervisor: João Barros. Co-supervisor: Rui Prior. Concluded: 07/2009.)
- **João Almeida**, Adaptive cryptography for Advanced Coding. (Supervisor: João Barros. Co-supervisor: Miguel Coimbra. Concluded: 07/2009.)
- **André Sousa**, Analysis of colour and texture features of vital-stained magnification-endoscopy images for computer-assisted diagnosis of precancerous and cancer lesions. (Supervisor: Miguel Coimbra. Concluded: 07/2008)
- **Rui A. Costa**, Capacity and Connectivity of Wireless Networks. (Supervisor: João Barros. Concluded: 10/2007)
- **João Paulo Vilela**, Cooperative Security Schemes for Optimized Link State Routing in Mobile Ad-hoc Networks. (Supervisor: João Barros. Concluded: 02/2007.)

Fellowships and Awards

João Barros

- Best Student Award, University of Porto, scholarship of merit, academic year 1997/1998.
- Socrates/Erasmus Scholarship from the EU, Karlsruhe, Germany, 1997/1998.
- Scholarship by the German Academic Exchange Service (DAAD), one-year graduate studies in Germany, not accepted due to full-time contract with TUM, July 1999.
- Essay Prize by the Japanese Foreign Ministry, 3-week study trip to Japan, September 1999.
- Fulbright Scholarship Award for a six-month research project at Cornell University.
- Best Teaching Award from the Bavarian State Ministry of Science, Research and the Arts, EUR 5000 , 2003.
- Sabbatical Fellowship from the Luso-American Foundation to help fund an 8-month research leave at MIT in 2008.

Miguel Rodrigues

- Prize Engenheiro António de Almeida.
- Prize Engenheiro Cristiano Spratley.
- Merit Scholarship from the University of Porto.
- Best student poster prize at the 2nd IMA Conference on Mathematics in Communications.
- Doctoral and postdoctoral fellowships from the Portuguese Foundation for Science and Technology.
- Postdoctoral fellowships from Foundation Calouste Gulbenkian.

Verónica Orvalho

- Winner 'AlumnIdea 2006' Organized by ALUMNI LEIC, FEUP Porto, Portugal.
- Finalist Award 'Innovact 2006' Organized by L'Etudiant ET L'Express.
- 3rd Place 'IV Concurso Innova 2004' Organized by UPC, EAE AND CIDEM Barcelona, Spain.
- Finalist Award 'Innovact 2004' organized by L'Etudiant ET L'Express.

Fausto Vieira

- Excellent Paper award - Fausto Vieira, M. A. Vázquez Castro, "Dynamic Price-based resource

allocation mechanism for ACM systems", 25rd International Communication Satellite Systems Conference (ICSSC 2007), Seoul, Korea, Apr. 2007.

- Best Paper award - A. Mayer, B. Collini-Nocker, F. Vieira, J. Lei, M.A. Vázquez Castro, "Analytical and Experimental IP Encapsulation Efficiency Comparison of GSE, MPE, and ULE over DVB-S2", International Workshop on Satellite and Space Communications, (IWSSC '07), Salzburg, Austria, pp. 114-118, 13-14 Sept. 2007.
- Young Graduate Trainee at the European Space Agency (ESA).
- Doctoral fellowship from the European Satellite Communications Network of Excellence (SatNEx) and from the ESA awarded contract on "IP-friendly cross-layer optimization of adaptive satellite systems".
- Postdoctoral contract within the "Ciência 2008" program from the Portuguese Foundation for Science and Technology.

Tiago Vinhoza

- Postdoctoral fellowship from the Portuguese Foundation for Science and Technology.
- Postdoctoral contract within the "Ciência 2008" program from the Portuguese Foundation for Science and Technology.
- Full Ph.D. Scholarship by the National Counsel of Technological and Scientific Development (CNPq), Brazil.
- Full M.Sc. Scholarship by the Coordination for the Improvement of Higher Education Personnel (CAPES), Brazil.
- Academic Excellence Certificate from PUC-Rio in 1999.

Tutorials and Talks

Tutorials and Talks in 2007

Miguel Rodrigues

- Secrecy rate of wiretap channels with arbitrary inputs. 3rd Workshop of the Thematic Network in Information Security, Porto, Portugal, December 2007.
- Optimum resource allocation in MIMO systems: An information theoretic-estimation theoretic approach. University College London, London, U.K., November 2007, Host: Izzat Darwazeh.
- Optimum resource allocation in MIMO systems: An information theoretic-estimation theoretic approach. University of Cambridge, Cambridge, U.K., November 2007, Host: Ioannis Chatzigeorgiou.
- Optimum resource allocation in MIMO systems: An information theoretic-estimation theoretic approach. Instituto Superior Técnico, Lisboa, Portugal, November 2007. Host: João Luís Sobrinho.
- Optimum power allocation for MIMO systems with discrete input distributions: An information theoretic-estimation theoretic approach. Bell Laboratories, Murray Hill, New Jersey, USA., September 2007. Host: Emina Soljanim.

Verónica Orvalho

- Invited Speaker, Fast and Reusable Facial Rigging and Animation, EA (Electronic Arts Europe), London, United Kingdom, October 24th 2007.
- Invited Speaker, Fast and Reusable Facial Rigging and Animation, UCL (University College London), London, United Kingdom, October 23rd 2007. external link [news external link]
- Invited Speaker, Videogame Development for Microsoft XNA Platform, Microsoft, Tagus Park, Portugal, October 15th 2007. [news external link]
- Workshop (24h), Videogame Design and Development, FCUP (Faculdade de Ciências da Universidade do Porto), Porto, Portugal, June 25th-27th 2007.
- Invited Speaker, Facial Synthesis and The Medical Industry, FCUP (Faculdade de Ciências da Universidade do Porto), Porto, Portugal, June 16th 2007.
- Invited Panelist, PhD Symposium for the PRESENCCIA project, UPC (Universitat Politècnica de Catalunya), Barcelona, Spain, May 2007. external link
- Invited Speaker, A Facial Animation System for CG Films and Videogames, FCUP (Faculdade de Ciências da Universidade do Porto), Porto, Portugal, February 26th 2007.
- Invited Speaker, A Facial Animation System for CG Films and Videogames, FEUP (Faculdade de Engenharia da Universidade do Porto), Porto, Portugal, February 27th 2007.

Tutorials and Talks in 2008

João Barros

- Information-theoretic Security: Theory and Practice. Tutorial presented at the IEEE International Symposium on Information Theory, Toronto, July 6, 2008.

Miguel Rodrigues

- Optimum power allocation for MIMO systems with discrete input distributions: An information theoretic-estimation theoretic approach. Mit-

subishi Electric Research Laboratories, Boston, Massachussets, USA., November 2008. Host: Simon Pun.

- Filter design with secrecy constraints. 4th Workshop of the Thematic Network in Information Security, Aveiro, Portugal, November 2008.
- Optimum power allocation for MIMO systems with discrete input distributions: An information theoretic-estimation theoretic approach. University of A Coruña, A Coruña, Spain, November 2008. Host: Luís Castedo.
- Filter design with secrecy constraints. Optimização e Redução de Ordem, Encontro de Laboratórios Associados - Ciência 2008, Fundação Calouste Gulbenkian, Lisbon, Portugal, July 2008.
- Information-theoretic security in wireless networks: From theory to practice. University of Plymouth, Plymouth, U.K., June 2008. Host: Martin Tomlinson.
- Information-theoretic security in wireless networks: From theory to practice. University College London, London, U.K., June 2008. Host: Ersi Chorti.
- Filter design with secrecy constraints. University of Cambridge, Cambridge, U.K., June 2008. Host: Ioannis Chatzigeorgiou.
- Filter design with secrecy constraints. Instituto Superior Técnico, Lisbon, Portugal, April 2008. Host: João Xavier.
- Optimum power allocation for MIMO systems with discrete input distributions: An information theoretic-estimation theoretic approach. Carnegie Mellon University, Pittsburgh, Pennsylvania, USA., March 2008. Host: José Moura.

Miguel Coimbra

- ”Medical Imaging Research @ NIP.”, UNICENTRO - Universidade Estadual do Centro-Oeste, Guarapuava, Brazil, July 2008.
- ”Medical Imaging Research @ NIP”, Real Hospital Português de Beneficiência de Pernambuco, Recife, Brazil, June 2008
- ”Applied Computer Vision Applications”, Fraunhofer Institute, Porto, July 2008.
- ”Applied Computer Vision Applications”, IBMC, Porto, January 2008.
- ”Analysis tools for endoscopic capsule exams”, MSc Seminar (MAOPI), FCUP, Porto, January 2008.

Verónica Orvalho

- Invited Speaker, Character Animation for Films and Videogames: Past, Present and Future, Seminario MTAD , Minho University, Guimarães, Portugal, November 21st 2008.
- Invited Speaker, New Trends on Character Animation, Digital Games’08 , Porto, Portugal, November 6th-7th 2008.
- Invited Speaker, New Trends on Character Animation, SHiFT 2008 , Lisbon, Portugal, October 15th-17th 2008.
- Workshop (35h), Videogame Design and Development for XNA, Microsoft, Lisbon, Portugal, March, 2008.
- Invited Speaker, Facial Animation for Films and Videogames a new Approach, VI Jornadas Computação Gráfica e Multimédia’08 , Viana do Castelo, Portugal, February 21th 2008.
- Invited Speaker, Make Faces: Automatically Transfer Expressions Between Characters, Sony, Foster City, California, USA, January 22th 2008.
- Invited Speaker, Make Faces: Automatically Transfer Expressions Between Characters, 7th International Conference on Neuroesthetics, UC Berkeley, USA, January 19th 2008.

Tutorials and Talks in 2009

João Barros

- Network Information Theory: Principles and Applications. Presented at the 5th Euro-NGI Conference on Next Generation Internet Networks, July 2009, Aveiro, Portugal.

Miguel Rodrigues

- Filter design with secrecy constraints. NEWCOM++ Emerging Technologies Workshop: Physical Layer Security, University of Padova, Padova, Italy, September 2009.

- Communication, information and estimation. CMU-Portugal Conference - Session on Mathematics for Information and Communication, Palácio da Bolsa, Porto, Portugal, June 2009.
- Optimal linear precoding for ergodic fading MIMO channels with discrete input distributions. University of Princeton, Princeton, N.J., USA., April 2009. Host: Sergio Verdú.
- Filter design with secrecy constraints. University of Delaware, Delaware, USA., April 2009. Host: Meritxell Lamarca.
- Optimum power allocation for MIMO systems with discrete input distributions: An information theoretic-estimation theoretic approach. University of Southampton, Southampton, U.K., February 2009. Host: Lajos Hanzo.
- Filter design with secrecy constraints. University of Cambridge, Cambridge, U.K., February 2009. Host: Albert Guillén e Fàbregas.

Miguel Coimbra

- ”Computer Assisted Analysis of Emerging Gastroenterology Imaging Technologies”, MSc Seminar (MSc in Medical Physics), FCUP, Porto, April 2009.
- ”Image Processing and Analysis”, 1st Basic Course on Optical Microscopy Imaging for Biosciences, IBMC, Porto, March 2009.
- ”Looking In: Emerging Imaging Technologies for Gastroenterology”, MSc Seminar (MIM), FMUP, Porto, March, 2009
- ”A Little Vision for Biologists”, MIT, Boston, USA, January 2009
- ”Vital Responder - Monitoring Stress in First Responder Professionals”, Carnegie-Mellon University, Pittsburgh, USA, January 2009.

Verónica Orvalho

- Invited Speaker, Research with XNA Technology, Microsoft Dev Days ’09 , Instituto Superior Tecnico, Lisbon, Portugal, February 18th-19th 2009.

Technical Services

Technical Services

João Barros

- Academic Committees
  - PhD Committee, Rui Prior, Department of Computer Science, University of Porto, April 2007.
  - PhD Committee, Matthieu Bloch, Georgia Institute of Technology, USA, April 2008.
  - PhD Committee, Fadi Abi-Abdallah, Eurecom, France, December 2008.
  - MSc Committee, João Xavier, Department of Electrical and Computer Engineering, University of Coimbra.
  - MSc Committee, Ricardo Tiago, Department of Electrical and Computer Engineering, Universidade Nova de Lisboa
- General Co-Chair 2007/08 of the IEEE Information Theory Workshop (ITW 2008), in Porto, Portugal, sponsored by the IEEE Information Theory Society.
- Organizer and Chair of the Technical Program Committee
  - First International Workshop on Information Theory for Sensor Networks (WITS 2007), held jointly with the IEEE Conference on Distributed Computing in Sensor Systems (DCOSS'07), Santa Fe, USA, June 2007.
  - Second International Workshop on Information Theory for Sensor Networks (WITS 2008), held jointly with the IEEE Conference on Distributed Computing in Sensor Systems (DCOSS'08), Santorini, Greece, June 2008. (Jointly with Aditya Ramamoorthy)
  - Third International Workshop on Information Theory for Sensor Networks (WITS 2009), held jointly with the IEEE Conference on Distributed Computing in Sensor Systems (DCOSS'09), Marina Del Rey, California, June 2009. (Jointly with Sandeep Pradhan)
- Member of the Technical Program Committee
  - IEEE Global Telecommunications Conference (IEEE GLOBECOM 2009), Adhoc and Sensor Networks Symposium.
  - IEEE Global Telecommunications Conference (IEEE GLOBECOM 2008), Communications Theory Symposium.
  - IASTED International Symposium on Distibuted Sensor Networks (DSN 2008), Orlando, USA, November 16, 2008 to November 18, 2008.
  - IASTED International Conference on Sensor Networks (SN 2008), Creta, Greece, September 29 - October 1, 2008.
  - IEEE Global Telecommunications Conference (IEEE GLOBECOM 2008), Ad-hoc and Sensor Networking Symposium.
  - International Workshop on Physics-inspired Paradigms in Wireless Communications and Networks Berlin, Germany, April 2008.
  - Information Theory and Statistical Learning' Conference (ITSL'08), held as part of WORLDCOMP' 08, the 2008World Congress in Computer Science, Computer Engineering, and Applied Computing in Las Vegas, Nevada (USA).
  - 6th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and

Wireless Networks (WiOpt 2008), sponsored by IEEE.

- IEEE Global Telecommunications Conference (IEEE GLOBECOM 2007), Ad-hoc and Sensor Networking Symposium.
- IEEE International Symposium on Information Theory (ISIT 2007) sponsored by the IEEE Information Theory Society.
- International Symposium on Information Security (IS'07), LNCS.
- 8th International Symposium on Systems and Information Security (SSI'2006), sponsored by the IEEE.
- 3a Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2007), Lisboa, Portugal.
- 4a Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2008), Coimbra, Portugal.
- 7th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt 2009), sponsored by IEEE.
- IEEE Information Theory Workshop (ITW 2009).
- 5th Euro-NGI on Next Generation Internet Networks (NGI 2008).
- 7th ConfTele, Aveiro, Portugal, May 2009.

- Session Chair
  - Member of the Organization Committee 2011/2012 for the IEEE International Symposium on Information Theory, Cambridge, MA, July 2012 (tutorial chair).
  - IEEE International Conference on Communications System, Guangzhou, China, November 2008 (Sessions: Network Architecture, Network Security and Cryptography, Wireless Mesh and Adhoc Networks)
  - Special Session on Network Security, Forty-Sixth Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sep. 2008.
  - IEEE International Conference on Information-Theoretic Security, Calgary, Canada, August 2008
  - IEEE International Symposium on Information Theory, Toronto, Canada, July 2008
  - IEEE International Symposium on Information Theory, Nice, France, June 2007
  - Special Session on Information-Theoretic Security, Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sep. 2007. Workshop Organizer 2007
  - 3rd TheNIS Workshop (Thematic Network on Information Security), Porto, Portugal, December 2007.
  - 6th RTCM Workshop (Portuguese Thematic Network on Mobile Communications) held jointly with the 6th Conference on Telecommunications (ConfTele 2007), Peniche, Portugal, May 2007.
  - DAIDALOS Internal Training (of the European Integrated Project with the same name), Porto, Portugal, May 2007.

Miguel Coimbra

- Academic Committees
  - PhD Committee, Sílvia de Francesco, UA, 2009
  - PhD Committee, Pedro João Soares Rodrigues, UM, Dec 2008
  - MSc Committee, João Correia, DMA, FCUP, 2009
  - MSc Committee, Sérgio Lima, DETI, UA, Jan 2009
  - MSc Committee, Denis Roda Dos Santos, DETI, UA, July 2008
- Member of the Technical Program Committee
  - ICIAR 2009, International Conference on Image Analysis and Recognition, Halifax, Canada.
  - ICIAR 2008, International Conference on Image Analysis and Recognition, Póvoa de Varzim, Portugal.

  - SecTech 2008, International Conference on Security Technologies, Samui, Thailand.

Miguel Rodrigues

- Member of the Technical Program Committee
  - 2008 IEEE Vehicular Technology Conference-Spring, Singapore.
  - 2008 IEEE International Conference on Broadband Communications, Networks, and Systems, London, U.K.
  - 2008 IET Conference Wireless, Mobile, Multimedia Networks, Mumbai, India.
- Publications Chair
  - 2008 IEEE Information Theory Workshop, Porto, Portugal.

Information Theory Workshop (ITW'08)

The Information Theory Workshop (ITW) is one of the major venues for researchers working on the fundamentals of information theory. IT-Porto was responsible for organizing ITW'08, which celebrated the 60th anniversary of Claude Shannon's landmark paper. It was hosted at Palácio da Bolsa, an historic building that goes back to the end of the 19th century, located in the heart of the World Heritage Site of Porto. The following set of photographs is intended to highlight some of the moments of this memorable event.

Palácio da Bolsa.

ITW banner showing one of Shannon's most famous formulas.

João Barros and Anthony Ephremides.

Muriel Médard and David Forney.

Anthony Ephremides and Daniel Costello.

Nicholas Laneman, Matthieu Bloch and Andrew Thangaraj.

Emina Soljanin.

Some organizing committee members.

Arabian Room at Palácio da Bolsa.

ITW participants and organizers.