Network Coding and Reliable Communications

Academic and Research Staff
Professor Muriel Medard
Dr. Nadia Fawaz (postdoctoral fellow)
Dr. Marie-Jose Montpetit (research scientist)
Dr. Chris Ng (postdoctoral fellow)
Dr. Una-May O'Reilly (research scientist)
Dr. Lucille Sasatelli (postdoctoral fellow)

Visiting Scientists and Research Affiliates
Professor Joao Barros (University of Porto)
Professor Frank Fitzek (University of Aalborg)
Professor Parastoo Sadeghi (National University of Australia)
Dr. Ivana Maric (Stanford)
Mr. Christopher Chang (Caltech)
Mr. Janus Heide (Aalborg University)
Mr. Siva Kumar (University of Illinois Urbana-Champaign)
Ms. Luisa Lima (University of Porto)
Mr. Gerhard Maierbacher (University of Porto)
Mr. Paulo Vasco Falcao Martins De Oliveira (University of Porto)
Mr. Morten Pedersen (Aalborg University)
Mr. Khaled Soussi (Technical University Munich)
Mr. Mohit Thakur (Technical University Munich)
Mr. Danail Traskov (Technical University of Munich)
Mr. Joao-Paulo Vilela (University of Porto)

Graduate Students
Mr. Soheil Feizi-Khankandi
Mr. Sheng Jing
Ms. Minji Kim
Mr. Minkyu Kim
Mr. Anthony Kim
Mr. Daniel Lucani
Mr. Ali ParandehGheibi
Ms. Shirley Shi
Mr. Jay-Kumar Sundararajan
Mr. Ramanathan Thinniyam
Mr. Guy Weichenberg
Ms. Fang Zhao

Professor Médard's group works extensively on capacity, in collaboration with CSAIL, LIDS, Caltech, the University of Illinois Urbana-Champaign (UIUC), UCLA, Stanford, the University of Porto, the University of Aalborg, Northeastern University and the Technical University of Munich (TUM). Network coding provides cost benefits in a variety of settings, for instance, wireless networks, where the cost may be measured in expended energy, or wireline networks, where they reduce congestion. In the area of network coding for wireless networks, she, Professor Katabi and Professor Ozdaglar have a DARPA contract through BAE to apply network coding to mobile ad-hoc networks (MANET) – CBMANET CONCERTO. The first phase of this contract has been very successful and this next phase concentrates on technology transfer to the warfighter. She has considered algorithmic issues of network coding in MANETs through the Army Research Office DAWN program, for which she is the sole MIT PI, in collaboration with University of California Santa Cruz, Stanford, University of Maryland College Park and University of California Los Angeles. In the area of network coding security, she is PI of a DARPA program and of an AFOSR program with Caltech and the University of Illinois Urbana-Champaign for the application of network coding to protect data under eavesdropping and Byzantine attacks. She is also MIT PI of a DARPA program through BAE for intrinsically assured MANETs (IAMANET PIANO), with University of Massachusetts Amherst, Stanford and University of Texas at Austin. She

investigates the general applicability of network coding to wireless systems through a NSF contract with Professor Katabi on XORs in the air.

In the area of information theory, Professor Medard has obtained, with Professors Ozdaglar, Shah and Zheng, a DARPA contract for the study of information theory for MANETs (ITMANET) with UIUC, TUM, Stanford and Caltech. This work has led to work on multiple access power control, distributed functional compression and analog network coding. She has also investigated fundamental coding issues in network coding through an NSF ITR project with Caltech, UIUC and Alcatel/Lucent Bell Laboratories.

Professor Medard also works in the area of optical network performance, reliability and robustness. With Professor Chan, she conducts research in the area of optical network capacity and optical access networks through an NSF FIND contract. Under the DARPA FONA project for optical networks, she and Professor Chan are investigating the limits of reliability of optical networks.

Professor Medard has also explored new areas at the intersection of communications and biochemistry for genomics and spectroscopy in collaboration with the Broad Institute and the Department of Chemistry.

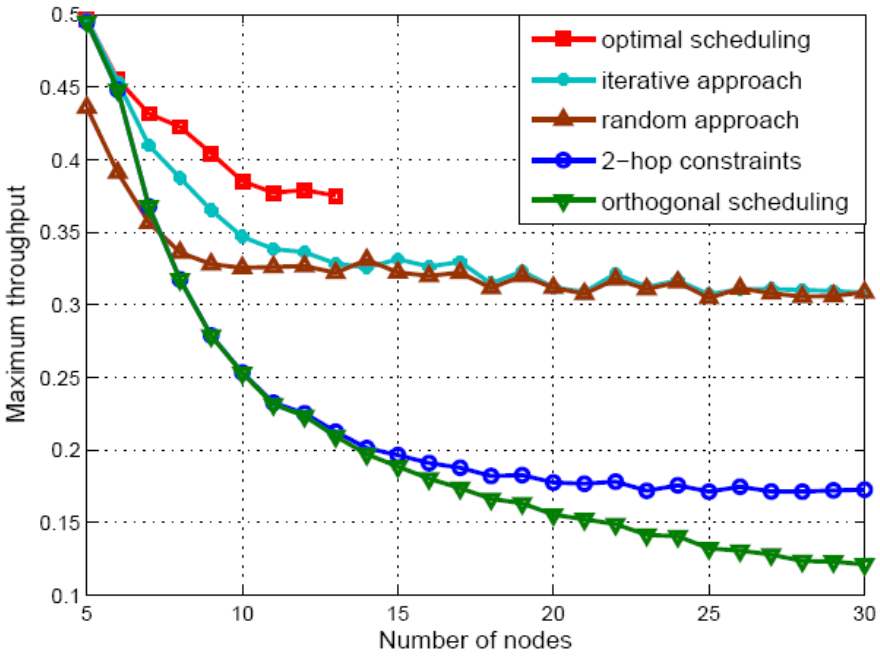
1. Information Theory for MANETs

Sponsor:
DARPA ITMANET under the FLOWS project

The purpose of this project is to investigate the information-theoretic limits of MANETs. The intrinsic limits consider topology, bandwidth, delay, capacity and energy.

As part of this project, we have considered, with the late Professor Koetter of the technical University of Munich and Professor Effros of Caltech, a theory of network equivalence. Given a network of noisy, independent, memoryless links, a collection of demands can be met on the given network if and only if it can be met on another network where each noisy link is replaced by a noiseless bit pipe with throughput equal to the noisy link capacity. This result subsumes previous separation results in the special case of multicast demands but does so without resorting to calculating capacity regions since that approach is infeasible for our more general problem. This claim has a number of surprisingly powerful consequences. Not only would it show separation between channel and network coding for arbitrary networks and arbitrary demands, also, many network information theoretic questions are naturally asked in the light of this combinatorial perspective. For example, the classical result that feedback does not increase the capacity of a point-to-point link now can be proven in two ways. The first is the information theoretic argument that shows that the channel has no information that is useful to the transmitter that the transmitter does not already know. The second simply observes that the min-cut between transmitter and receiver is the same with or without feedback, which is obvious from the given equivalence. Most importantly, this statement reveals that at the heart of information theory lie combinatorial problems involving finding the rate region for error-free networks.

We also consider, with the late Professor Koetter and his students, the issue of network capacity in the context of scheduling. Traditional techniques have sought to preclude interference in networks, by attempting to maintain orthogonality in transmissions. We address the problem of maximizing the throughput for network coded multicast traffic in a wireless network in the bandwidth limited regime. For the joint scheduling and subgraph selection problem, we model valid network configurations as stable sets in an appropriately defined conflict graph. The problem formulation separates the combinatorial difficulty of scheduling from the arising optimization problem and facilitates the application of less complex scheduling policies. Lagrangian relaxation gives rise to a distributed algorithmic solution when combined with greedy scheduling. Simulation results show that our technique is nearly optimal and outperforms heuristics such as orthogonal scheduling by a large margin.



Maximum throughput with network coded scheduling allowing better performance than orthogonal scheduling and approximate two-hop orthogonal scheduling.

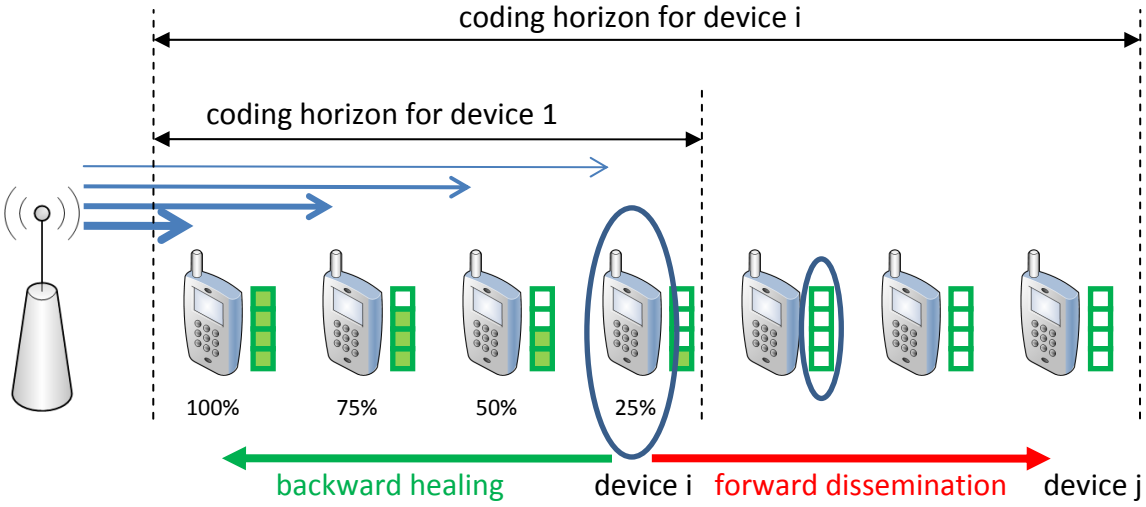
.

2. Practical approaches to wireless network coding

Sponsors:
NSF XORs in the air
DARPA CBMANET
ARO DAWN program

Wireless networks suffer from interference and, in some cases, considerable delay. We have considered how to create practical schemes that allow us to design network coding mechanisms in the context of wireless settings, so that physical layer issues are explicitly taken into account in the development of our codes. Such issues are of particular importance in MANETs, where the paucity of resources, the variability of the topology and the uncertainty in the channels render the physical layer effects particularly challenging.

With Professor Fitzek of University of Aalborg, Professor Milica Stojanovic of Northeastern University and our student, we propose a linear network coding scheme to disseminate a finite number of data packets in arbitrary networks. The setup assumes a packet erasure channel, slotted time, and that nodes cannot transmit and receive information simultaneously. The dissemination process is completed when all terminals can decode the original data packets. We also assume a perfect knowledge of the information at each of the nodes, but not necessarily a perfect knowledge of the channel. A centralized controller decides which nodes should transmit, to what set of receiver nodes, and what information should be broadcasted. We show that the problem can be thought of as a scheduling problem, which is hard to solve. Thus, we consider the use of a greedy algorithm that only takes into account the current state of the system to make a decision. The proposed algorithm tries to maximize the impact on the network at each slot, i.e. maximize the number of nodes that will benefit from the coded packet sent by each active transmitter. We show that our scheme is considerably better, in terms of the number of slots to complete transmission, than schemes that choose the node with more information as the transmitter at every time slot.



Network coding dissemination through the node with most impact rather than the node with the most degrees of freedom.

One of the concerns in the implementation of network coding is the complexity associated with using coding over fields larger than two. With Professor Stojanovic and our student, we study the effect of the field size on the performance of random linear network coding for time division duplexing channels we have previously proposed. In particular, we study the case of a node broadcasting to several receivers. We show that the effect of the field size can be included in the transition probabilities of the Markov chain model of the system. Also, we have derived an improved upper bound on the mean number of coded packets required to decode M original data packets using random linear network coding. This bound shows that even if the field size is 2, i.e. we perform XORs amongst randomly selected packets from the pool of M original ones, we will need on average at most M+2 coded packets in order to decode. Thus, there will be only a very small degradation in performance if M is large. Our numerical results show that the mean completion time of our scheme with a field size of 2 is close in performance to our scheme when we use larger field sizes. We also show that as M increases, the difference between using a field size of 2 and larger field sizes decreases. Finally, we show that we can get very close to the optimal performance with small field sizes, e.g. a field size of 4 or 8, even when M is not very large.

3. Security aspects of network coding

Sponsors:
DARPA IAMANET program

Network coding provides new possibilities for security but also poses new challenges for traditional security techniques.

With Professor Barros of Porto and our student, we propose a scheme, called the algebraic watchdog for wireless network coding, in which nodes can detect malicious behaviors probabilistically, police their downstream neighbors locally using overheard messages, and, thus, provide a secure global self-checking network. Unlike traditional Byzantine detection protocols which are receiver based, this protocol gives the senders an active role in checking the node downstream. This work is inspired by Marti et al.'s watchdog-pathrater, which attempts to detect and mitigate the effects of routing misbehavior. We develop a graphical model to understand the inference process nodes execute to police their downstream neighbors; as well as to compute, analyze, and approximate the probabilities of misdetection and false detection. In addition, we create an algebraic analysis of the performance using an hypothesis testing framework, that provides exact formulae for probabilities of false detection and misdetection.

Network coding's high throughput in settings with high erasure probabilities renders it particularly attractive for wireless video transmission. With Professor Barros and his students, we have created SPOC (Secure Practical Network Coding), which introduces a new paradigm for security in network coding: instead of encrypting the file directly, encryption is performed at the network coding layer. This paradigm offers striking advantages in comparison with end-to-end encryption of the data, especially for multimedia and streaming applications, where the number of cryptographic operations can become prohibitive. In this work, we evaluate and extend this paradigm for (1) delay sensitive applications and (2) successive refinement applications in which nodes have distinct levels of access to data. As part of our contribution, we present an information theoretic security analysis of the schemes, considerations on system aspects and simulations for wireless multimedia networks.

4. Optical networks

Sponsors:
DARPA FONA

Providing resilient service against failures is a crucial issue for today's optical networks because they operate at very high data rates and thus a single failure may cause a severe loss of data. A variety of protection techniques have been extensively studied for the fault-tolerant operation of optical networks of either ring or mesh topologies. Among them, we particularly focus on the path protection scheme with live back-up, which provides extremely fast recovery, requiring action only from the receiving node. A conventional way to implement such a protection scheme is to transmit two live flows, a primary and a back-up, along link-disjoint paths so that upon link failure the receiver node can switch to the back-up flow. However, it may require an excessive amount of redundant capacity as back-up capacity is not shared among connections. Recent developments have demonstrated that network coding can lead to significant savings in the back-up resources for the multicast scenario protected against link failure by live back-up. An unique and crucial characteristic of optical networks is converting photonic streams into electronic signals for data processing (O/E/O conversion) is an expensive procedure. Since arbitrary coding operations must be performed in the electronic domain, it appears sensible to restrict the coding operations only to bitwise XOR, which can be done within the optical domain using a photonic bitwise

5. Managing on degrees of freedom

Sponsors:
AFOSR

We consider the issue of making optimal use of degrees of freedom when we have joint computation, source coding and network coding.

With Professor Barros and our student, we consider the ability perform network coding and source coding jointly, which When correlated sources are to be communicated over a network to more than one sink, joint source-network coding is, in general, required for information theoretically optimal transmission. Whereas on the encoder side simple randomized schemes based on linear codes suffice, the decoder is required to perform joint source-network decoding which is computationally expensive. Focusing on maximum a-posteriori decoders (or conditional mean estimators, in the case of continuous sources), we show how to exploit (structural) knowledge about the network topology as well as the source correlations giving rise to an efficient decoder implementation (in some cases even with linear dependency on the number of nodes). In particular, we show how to statistically represent the overall system (including the packets)by a factor-graph on which the sum-product algorithm can be run. We provide a proof-of-concept in the form of a working decoder for the case of three sources and two sinks.

With my student, we consider a tree network with k possibly correlated source processes in its leaves and a receiver in its root wishes to compute a deterministic function of these processes. Other nodes in this tree (called intermediate nodes) can compute some functions in demand. We want to find feasible rates for different links of this tree network (called the rate region of this network) and propose a coding scheme to achieve these rates. We only consider the lossless computation of the function.This problem was an open problem in general. But, for some simple networks under some special conditions, it has been solved. For instance, our previous work considered the rate region of a network with two transmitters and a receiver, under a condition on source random variables called the zigzag condition. The zigzag condition forces source sequences to be mostly jointly typical. Our work extends the previous results in two senses: first, we consider an arbitrary tree network with some intermediate nodes which are allowed to compute some functions, and second, we compute the rate region without considering any conditions. To do this, we define the joint graph entropy of some random variables and use it in our results. In some special cases, this general definition can be simplified to previous definitions proposed in our previous work. We also propose a framework to categorize different tree network topologies by using some concepts like auxiliary nodes, stage, etc. Our results show that for any tree network, it is sufficient for source nodes to compute minimum entropy colorings of their high probability subgraphs of their characteristic graphs satisfying a necessary and sufficient condition, which we term the coloring connectivity condition (C.C.C.), and then, to perform Slepian-Wolf compression. The intermediate nodes in the network may act like relays. Such a scheme, in which all processing is effected at the sources, can perform arbitrarily closely to the derived rate region with a vanishing probability of error at the receiver.

Publications

Journal articles, accepted for publication

1. S. Jing, Zheng, L., and Médard, M., “On Training with Feedback in Wideband Channels”, *IEEE Journal on Selected Areas in Communications: Special Issue on Limited Feedback*, Volume 26, Issue 8, October 2008, pp:1607 - 1614**
2. L. D. Jennings, Lun, D. S., Médard, M., and Licht, S. “ClpP Hydrolyzes a Protein Substrate Processively and Independently with Respect to the ClpA ATPase: Mechanistic Studies of ATP-Independent Processive Proteolysis”, *Biochemistry,* 47(44):11536-11546, November 2008
3. A. Eryilmaz, Ozdaglar, A., and Médard, M., “On the Delay and Throughput Gains of Coding in Unreliable Networks”, *IEEE Transactions on Information Theory*, Volume 54, Issue 12, December 2008, pp:5511 - 5524
4. D. Lucani, Stojanovic, M., and Médard, M., “Channel Models and Network Coding based Lower Bound to Transmission Power for Multicast”, *IEEE Journal on Selected Areas in Communications: Special Issue on Underwater Acoustic Networks*, Volume 26, Issue 9, December 2008, pp:1708 - 1719**
5. P. Youssef-Massaad, Zheng, L., and Médard, M., “Bursty Transmission and Glue Pouring: on Wireless Channels with Overhead Costs”, *IEEE Transactions on Wireless Communications,* Volume 7, Issue 12, Part 2, December 2008, pp:5188 - 5194 **
6. G. Weichenberg, Chan, V., and Médard, M., “Design and Analysis of Optical Flow Switched Networks” accepted to the *IEEE Journal of Optical Communications and Optical Networking***

Meeting papers, published

7. S. Katti, Katabi, D., Balakrishnan, H., and Médard, M., “Symbol Level Network Coding for Wireless Mesh Networks”, *Sigcomm,* August 2008
8. A. ParandehGheibi, Eryilmaz, A. Ozdaglar, A., and Médard, M., “Information Theory vs. Queueing Theory for Resource Allocation in Multiple Access Channels”, **invited** paper, *PIMRC*, September 2008**

9. S. Jing, Zheng, L., and Médard, M., “Layered Source-Channel Coding: Towards Unifying Multiple Description and Successive Refinement”, **invited** paper, *Allerton Conference*, October 2008**
10. M. Kim, Médard, M., O’Reilly, U.-M., “Integrating Network Coding into Heterogeneous Wireless Networks”, *MILCOM*, November 2008** (9.3)
11. M. Kim, Médard, M., Barros, J., “Counteracting Byzantine Adversaries with Network Coding: An Overhead Analysis”, *MILCOM*, November 2008** (9.5)
12. D. Lucani, Médard, M., and Stojanovic, M., "A Lower Bound to Transmission Power for Multicast in Underwater Networks using Network Coding", accepted to *ISITA*, December 2008**
13. J.-K. Sundararajan, Shah, D., and Médard, M., “Online Network Coding for Optimal Throughput and Delay – the Three-Receiver Case”, *ISITA*, December 2008**
14. L. Lima, Barros, J., Vilela, J.-P., and Médard, M., “An Information-Theoretic Cryptanalysis of Randomized Network Coding - is Protecting the Code Enough?”, *ISITA*, December 2008
15. D. Traskov, Heindlmaier, M., Médard, M., Koetter, R. and Lun, D.S., “Scheduling for Network Coded Multicast: A Conflict Graph Formulation”, *4th IEEE Workshop on Broadband Wireless Access*, December 2008
16. D. Lucani, Médard, M. and Stojanovic, M. , “On Coding for Delay: New Approaches Based on Network Coding in Networks with Large Latency”, **invited paper**, *ITA conference*, February 2009
17. D. Lucani, Médard, M. and Stojanovic, M. , “Random Linear Network Coding for Time Division Duplexing: When to Stop Talking and Start Listening”, *INFOCOM 2009,* April 2009**
18. M. Kim, O’Reilly, U.-M., Médard, M. and Traskov, D., “An Evolutionary Approach To Inter-Session Network Coding”, *INFOCOM 2009,* April 2009**
19. J.-K. Sundararajan, Shah, D., Médard, M., Mitzenmacher, M, Barros, J. “Network Coding Meets TCP”, *INFOCOM 2009,* April 2009**
20. D. Lucani, Médard, M. and Stojanovic, M. , “Random Linear Network Coding For Time Division Duplexing: Energy Analysis”, *ICC Communication Theory Workshop*, June 2009**
21. C. Ng, Médard, M. and Ozdaglar, A., “Completion Time Minimization and Robust Power Control in Wireless Packet Networks”, *ICC Communication Theory Workshop*, June 2009
22. D. Lucani, Médard, M. and Stojanovic, M. , “Completion Time Minimization and Robust Power Control in Wireless Packet Networks”, accepted to *ICC Communication Theory Workshop*, June 2009**
23. G. Weichenberg, Chan, V.W.S. and Médard, M., “Performance Analysis of Optical Flow Switching”, *ICC Optical Networks,* June 2009**
24. R. Koetter, Effros, M. and Médard, M., “On a theory of network equivalence”, accepted to *Information Theory Workshop*, June 2009
25. D. Lucani, Fitzek, F., Médard, M. and Stojanovic, M., “Network Coding For Data Dissemination: It Is Not What You Know, But What Your Neighbors Don’t Know”, **invited** paper, *RAWNET*s, June 2009**
26. J.-K. Sundararajan, Sadeghi, P. and Médard, M., “A feedback-based adaptive broadcast coding scheme for minimizing in-order delivery delay”, *Netcod*, June 2009**
27. D. Lucani, Médard, M. and Stojanovic, M., “Broadcasting in time-division duplexing: A random linear network coding approach”, *Netcod*, June 2009**
28. M. Kim, Médard, M., Barros, J. and Koetter, R., “An Algebraic Watchdog for Wireless Network Coding”, *ISIT*, July 2009**
29. D. Lucani, Médard, M. and Stojanovic, M., “Random Linear Network Coding for Time-Division Duplexing: Queueing Analysis”, *ISIT*, July 2009**
30. G. Maierbacher, Barros, J., and Médard, M., “Practical Source-Network Decoding”, **invited** paper, accepted to *IEEE International Symposium on Wireless Communication Systems*, 2009
31. D. Lucani, Médard, M. and Stojanovic, M., “Random Linear Network Coding for Time-Division Duplexing: Field Size Considerations”, accepted to the *IEEE Globecom 2009 Communication Theory Symposium***

32. D. Traskov, Médard, M., Sadeghi, P. and Koetter, R., "Joint Scheduling and Instantaneously Decodable Network Coding", accepted to the *IEEE Globecom 2009 Communication Theory Symposium*
33. S. Feizi, and Médard, M., "Multi-Functional Compression with Side Information", accepted to the *IEEE Globecom 2009 Communication Theory Symposium*
34. S. Feizi and Médard, M., "Only Sources Need to Compute, On Functional Compression in Tree Networks", accepted to the *2009 Annual Allerton Conference on Communication, Control, and Computing***
35. D. Lucani, Médard, M. and Stojanovic, M., "Sharing Information in Time-Division Duplexing Channels: A Network Coding Approach", accepted to the *2009 Annual Allerton Conference on Communication, Control, and Computing***
36. M Langberg and Médard, M., "the Multiple Unicast Network Coding Conjecture", accepted to the *2009 Annual Allerton Conference on Communication, Control, and Computing*

Meeting paper, presented

September 2007, "Le codage sur réseaux - théorie, applications et nouvelles frontières", **Plenary Speaker**, GRETSI 2007, Troyes, France

September 2007, "New Directions in Wireless Communications," **Gilbreth Lecture** to the National Academy of Engineering

January 2008, "On Theory and Practice in Network Coding", **Keynote Lecture**, Coordinated Science Laboratory at UIUC 3rd annual Student Conference in the areas of Control, Communications and Signal Processing.

February 2008, "Delay and throughput in network coding", **invited** seminar, Iowa State University

June 2008, "Network Coding", **invited** course, First School of Information Theory, organized by the IEEE Information Theory Society at Penn State

June 2008, "Network coding and security", **Keynote Address,** IEEE Workshop on Wireless Network Coding, San Francisco

June 2008, "An Introduction to Network Coding", short course given at Bretagne Telecom, France

June 2008, "Le codage sur réseaux – principes et applications", **invited** lecture, at the PRACOM conference, Bretagne Telecom

Theses

Doshi, Vishal, "Functional Compression: Theory and Applications", February 2008 (co-supervised with Devavrat Shah)

ParandehGhebi, Ali, "Fair Resource Allocation in Multiple AccessChannels", June 2008 (co-supervised with Asuman Ozdaglar)