Workshop on Information Theory and Applications
June 1, 2010 - FEUP Room I322
Program

9h30-9h50 - João Barros, *IT Porto Intro*

9h50-10h50 - Imre Csiszár, *On Mathematical Foundations of Information Theoretic Secrecy*

Information theoretic secrecy is a rapidly developing field of information theory. It offers provable and unconditional security for a variety of cryptographic tasks, of which we will concentrate on secure communication over insecure channels, and generating a secret key taking adventage of public communication. A main mathematical concept for these problems is Common Randomness (CR) which becomes a Secret Key (SK) if concealed from unauthorized parties. To establish foundamental limits for generating CR and SK in various models, including both source and channel models, a main mathematical tool is the Extractor Lemma. Another important tool, for proving converse results, is an algebraic identity for mutual information that comes from multiuser information theory. This talk will survey some basic issues along these lines.

10h50 - 11h10 - Coffee Break

11h10-11h30 - Vinay Prabhu, *On Physical Layer Secrecy in Slow Fading Wireless Systems with Multiple Antennas*

We consider an opportunistic secrecy-achieving scheme in wireless slow-fading environs that targets secure communications over a 'main channel' existent between a transmitter and a legitimate receiver in the presence of an 'eavesdropper channel' existent between the transmitter and the eavesdropper. Here, the transmitter transmits data to the intended receiver only when the main channel SNR is greater than the eavesdropper channel SNR at a maximum rate equal to the difference between the main channel and the eavesdropper channel capacities. In our work, we

analyse the effect levied on the critical secrecy parameters, namely the probability of existence of secrecy capacity, the secrecy outage probability and ϵ-outage secrecy capacity when:

1: There are multiple eavesdroppers or eavesdroppers with multiple antennas.

2: There exists a LOS path between the eavesdropper(s) and the transmitter.

3: The legitimate receiver can afford receive diversity with MRC and SDC reception.

4: There exists spatial correlation in case of multiple antennas at either the main receiver or the eavesdropper.

11h30 - 11h50 - João Almeida, *Joint Cryptography and Data Compression*

In this talk we will address the design of source encoders with encrypted output. Building on the parallel between key-streams and error patterns, we propose an encoding scheme that leverages on induced catastrophic errors to achieve message confidentiality. The output of such encoder is a pair of streams consisting of a cryptogram and respective key-stream. Using synchronization arguments, we design algorithms that compute these pairs with highly compressible key-streams. This is a desirable property since, generally we will employ stronger cryptographic primitives on top of these schemes. By assuring compressible key-streams we remarkably reduce the additional computational effort of using state-of-the-art cryptography.

11h50 - 12h10 - Gerhard Maierbacher, *Scalable Coding Solutions for Wireless Sensor Networks*

Considering a sensor network scenario where correlated data from potentially large number of independently operating sensors has to be communicated to one or several sinks, the need for computationally tractable joint source-network coding solutions arises. In this talk we present some methodologies to overcome complexity problems associated with the code design and the encoder/ decoder implementations for large-scale scenarios. In order to provide a scalable coding solution, i.e. a solution that is feasible for an arbitrarily large number of sensors, we propose methods based on source-optimized clustering and factor-graph decoding that achieve attractive trade-offs between complexity and system performance. In particular, we address the problem of finding correlation preserving clusters using the Kullback Leibler Distance as optimization criterion and show how to statistically represent the overall

system by a factor-graph on which the sum-product algorithm can be run for an efficient decoder implementation.

12h10 - 12h30 - Mari Nistor, *Non-Asymptotic Analysis of Network Coding Delay*

We present an expression for the delay distribution of Random Linear Network Coding over an erasure channel with a given loss probability. In contrast with previous contributions, our analysis is non-asymptotic in the sense that it is valid for any field size and any number of symbols. The results confirm that GF(16) already offers near-optimal decoding delay, whereas smaller field sizes (e.g. requiring only XOR operations) induce heavy tails in the delay distribution. A comparison with Automatic Repeat reQuest (ARQ) techniques (with perfect feedback) is also included.

12h30 - 14h00 - Lunch

14h00 - 15h00 - Prakash Narayan, *Secrecy and Tree Packing*

This talk addresses connections between the information theoretic notion of multiterminal secrecy and the combinatorial notion of tree packing.

Consider a situation in which multiple terminals observe separate but correlated signals and a subset of these terminals seek to devise a secret key through public communication that is observed by an eavesdropper, in such a way that the key is concealed from the eavesdropper. We show how this problem is connected to a multiterminal data compression problem (without secrecy constraints), and illustrate the connection with a simple key construction. Next, for a special "pairwise independent network model," of relevance to wireless communication, in which every pair of terminals observes correlated signals that are independent of the signals observed by all other pairs of terminals, we show a natural connection between secrecy generation and a (separate) combinatorial problem of maximal packing of Steiner trees in an associated multigraph. This talk is based on joint works with Imre Csiszar, Sirin Nitinawarat, Chunxuan Ye, Alexander Barg and Alex Reznik.

15h00 - 15h30 - Daniel Lucani, *(Network) Coding for Uncertain Networks*

This talk discusses different sources of uncertainty in networks, the challenges they pose, and proposes network coding approaches to assess these challenges. In particular, we consider four, possibly interrelated, sources of uncertainty in networks: channel, delay, interference, and rate. In networks with packet losses (channel uncertainty) and large latency (delay), feedback about received packets may lag considerably the transmission of the original packets, limiting the feedback's usefulness. Moreover, half duplex constraints may entail that receiving feedback may be costly. In this talk, we consider tailoring feedback and coding jointly in such settings to reduce the expected delay for successful in order reception of packets. We find that, in certain applications, judicious choices provide results that are close to those that would be obtained with a full-duplex system. We also discuss other interesting topics in networks with uncertainty. For example, we discuss an efficient distributed algorithm for performing inter-layer coding for multicasting data to users that have different (potentially time-varying) rate limitations/expectations, which is a case of rate uncertainty.

15h30 - 16h00 - Tiago T. V. Vinhoza, *Impact of Vehicles as Obstacles in Vehicular Ad hoc Networks*

There exists a considerable body of work on channel modeling for vehicular ad-hoc networks (VANET). Although line of sight (LOS) is generally considered to be important, the impact of vehicles as obstacles on LOS communication has been largely ignored. A suitable model for VANET that accounts for this aspect must satisfy a number of conditions, such as accurate positioning and mobility patterns of vehicles, realistic propagation characteristics, and manageable complexity. We present a model that satisfies all of these conditions. We model vehicles as physical obstacles in order to evaluate how they affect vehicle-to-vehicle (V2V) communication. We develop a channel model that includes these new obstacles and evaluate their impact on the received signal power and the packet reception rate. We analyze both highway and urban scenarios based on the real world data collected via stereoscopic aerial photography. The results show significant attenuation and packet loss caused by vehicles as obstacles. The algorithm behind the proposed model allows for computationally efficient implementation in VANET simulators and we show that it could add realism to simulations with implications on upper layer protocol design

16h00 - 16h20 - Coffee Break

16h20 - 16h40 - João Paulo Vilela, *Friendly Jamming for Wireless Secrecy*

We analyze the role of jamming as a means to increase the security of wireless systems. Specifically, we characterize the impact of cooperative/friendly jamming on the secrecy outage probability of a quasi-static wiretap fading channel. We introduce jamming coverage and jamming efficiency as security metrics, and evaluate the performance of three different jamming strategies that rely on various levels of channel state information. The analysis provides insight for the design of optimal jamming configurations and indicates that one jammer is not enough to maximize both metrics simultaneously.

16h40 - 17h00 - Hugo Reboredo, *Filter Design with Secrecy Constraints*

A communication system usually operates under limited resources such as the transmit power and the bandwidth. The efficient use of these resources constitutes a key element in the performance of communications systems. In order to maximize this performance one approach is to design optimal linear transmit filters according to some performance criteria subject to the set of constraints imposed by the limited resources and by some other additional requirements. In this talk, we consider the problem of filter design with secrecy constraints, where two legitimate parties (Alice and Bob) communicate in the presence of an eavesdropper (Eve), over a Gaussian multiple-input multiple-output (MIMO) wiretap channel. In particular, we consider the design of the transmit and the receive filters which, on the one hand, minimize the mean-squared error (MSE) between the legitimate parties and, on the other hand, assure that the eavesdropper MSE remains above a certain level. We consider both the case where the optimal receive filter corresponds to a Wiener filter, and the case where zero-forcing filters are used at the receivers, characterizing the optimal transmit filter and providing an algorithm to obtain its elements. Finally, we present a set of numerical results to support some of the main conclusions.

17h00 - 17h20 - Saurabh Shintre, *Rate-distortion Approach to Relevance*

Mathematical modeling of relevance turns into rate-distortion problem with per-letter criteria. We see if the solution remains the same, investigate the practical application of using such constraints and its advantages/disadvantages over the usual R-D theory.

17h20 - 17h40 - Rui Costa, *One-Shot Capacity of Discrete Channels*

Shannon defined channel capacity as the highest rate at which there exists a sequence of codes of block length n such that the error probability goes to zero as n goes to infinity. In this definition, it is implicit that the block length, which can be viewed as the number of available channel uses, is unlimited. This is not the case when the transmission power must be concentrated on a single transmission, most notably in military scenarios with adversarial conditions or delay-tolerant networks with random short encounters. A natural question arises: how much information can we transmit in a single use of the channel? We give a precise characterization of the one-shot capacity of discrete channels, defined as the maximum number of bits that can be transmitted in a single use of a channel with an error probability that does not exceed a prescribed value. This capacity definition is shown to be useful and significantly different from the zero-error problem statement.

17h40 - 17h50 - Closing Remarks