Signals, Information, and Algorithms

RLE Group
Signals, Information and Algorithms Laboratory

Faculty
Professor Gregory W. Wornell

Visiting Scientists and Research Affiliates
Dr. Uri Erez[1], Hiroyuki Ishii [2], Dr. Emin Martinian[3], Dr. Chen-Pang Yeang[4]

Postdoctoral Scholars
Dr. Aslan Tchamkerten

Graduate Students
Anthony Accardi, Lane Brooks, Venkat Chandar, Vijay Divi, Ying-Zong Huang, Ashish Khisti, Maryam Shanechi, Urs Niesen, Charles Swannack

Administrative Staff
Tricia Mulcahy

Introduction

Our laboratory formulates, examines, and develops algorithmic solutions to a wide spectrum of problems of fundamental interest involving the manipulation of signals and information in diverse settings. Our work is strongly motivated by and connected with emerging applications and technologies.

In pursuing the design of efficient algorithm structures, the scope of research within the lab extends from the analysis of fundamental limits and development of architectural principles, through to implementation issues and experimental investigations. Of particular interest are the tradeoffs between performance, complexity, and robustness.

In our work, we draw on diverse mathematical tools—from the theory of information, computation, and complexity; statistical inference and learning, signal processing and systems; coding and communication; and networks and queuing—in addressing important new problems that frequently transcend traditional boundaries between disciplines.

We have many joint projects and collaborate closely with faculty, staff, and students in a variety of other labs on campus, including the Laboratory for Information and Decision Systems, the Microsystems Technologies Laboratories, and Computer Science and Artificial Intelligence Laboratory.

Much of our activity over the last few years has centered around a variety of different types of problems arising naturally in the context of wireless, sensor, multimedia, and broadband networks.

---

[1] Department of Electrical Engineering, Tel-Aviv University, Israel
[2] NEC Corporation, Intelligence Systems Department, Tokyo, Japan
[3] Mitsubishi Electric Research Laboratories, Cambridge, Mass.
[4] University of Toronto, Toronto, Canada

Some topics of current interest include:

- cross-layer design techniques and architectural considerations for resource-efficient wireless networks
- coding for multiple-element antenna arrays in wireless networks, and interactions with other layers; advanced antenna designs
- new classes of source and channel codes, and decoding algorithms, particularly for new applications
- diversity techniques and interference suppression and management algorithms for wireless networks
- distributed algorithms and robust architectures for wireless networks, especially ad-hoc networks and sensor networks
- algorithms and fundamental limits for multimedia security problems, including digital watermarking, encryption, and authentication of multimedia content
- algorithms and architectures for multimedia and streaming media networks
- algorithmic and coding techniques for generating reliable advanced systems from aggressively scaled devices, circuits, and microsystems.
- information-theoretic and algorithmic aspects of learning, inference, and perception; universal algorithms
- information-theoretic and signal processing aspects of neuroscience, and computational and systems biology

Projects

1. Digital Processing in Imaging Systems

Sponsors
FCRP Center for Circuits and System Solutions, Contract No. 2003-CT-888
MIT Lincoln Laboratory

Project Staff
Anthony Accardi, J. Chu, K. Nguyen, J. Powell, H. Kim*, Professor Gregory Wornell, Professor Harry Lee, and Professor Charles Sodini
* MIT Lincoln Laboratory

Due to advances in silicon and digital processing technology, low-cost millimeter-wave (MMW) imaging solutions with high antenna array density are now viable. Meanwhile, research in computational photography has demonstrated how more information can be captured by cameras operating in the visible spectrum, redefining what it means to take a photograph. We are developing a framework that encompasses both types of imaging architectures, which allows us to translate advances in one regime to the other.

The light field, which represents radiance at each point in space along each direction, has proven to be a useful abstraction in computational photography. We generalize the light field to describe coherent illumination, and explore how to estimate the light field when direct field measurements are made with antennas. As an application, we specify how to take near-field pictures with an antenna array, so that one can programmatically adjust the virtual focus and f-stop.

Phase noise is a practical concern when processing signals with high frequency content. We explore how phase noise impacts imaging system performance, and propose a hybrid analog/digital phase-locked loop to reduce phase noise at each antenna.

2. Circuits and Algorithms for Pipelined ADCs in Scaled CMOS Technology

Sponsors
NDSEG Fellowship
CICS (Center of Integrated Circuits and Systems)

Project Staff
Lane Brooks, Professor Hae-Seung Lee, Professor Gregory Wornell

CMOS technology scaling is creating significant issues for analog circuit design. For example, reduced signal swing and device gain make it increasingly difficult to realize high-speed, high-gain feedback loops traditionally used in switched capacitor circuits. This research involves two complementary methods for addressing scaling issues. First is the development of two blind digital calibration techniques. Decision Boundary Gap Estimation (DBGE) removes static non-linearities and Chopper Offset Estimation (COE) nulls offsets in pipelined ADCs. Second is the development of circuits for a new architecture called zero-crossing based circuits (ZCBC) that is more amenable to scaling trends. To demonstrate these circuits and algorithms, two different ADCs were designed: an 8 bit, 200MS/s in TSMC 180nm technology, and a 12 bit, 50 MS/s in IBM 90nm technology. Together these techniques can be enabling technologies for both pipelined ADCs and general mixed signal design in deep sub-micron technologies.

3. The Impact of Asynchronism on Communication

Sponsors
University IR&D Grant from Draper Laboratory
DoD MURI N00014-07-1-0738

Staff
Venkat Chandar, Aslan Tchamkerten and Professor Gregory Wornell

This research addresses the question of how a lack of synchronization between the transmitter and the receiver affects the range of achievable communication rates. We handle this question by introducing a new discrete time asynchronous channel model for point-to-point communication. The transmitter may start to emit information at any moment within a certain time interval, representing the level of asynchronism, and the receiver must decode without knowing when transmission starts but being cognizant of the asynchronism level.

We have shown several results concerning the fundamental limits of communication under this model. In particular, we formulated a definition of rate suitable for the asynchronism model described above, and provided inner and outer bounds on the rate-asynchronism level region. We also analyzed several related, but easier problems. For example, we have determined a simple formula for the synchronization threshold, i.e., the maximum asynchronism level beyond which it is impossible to have reliable communication, even at zero rate.

4. Signal Recovery in Distributed Sampling Systems

Sponsors
MIT Lincoln Laboratory
FCRP Center for Circuits and System Solutions, Contract No. 2003-CT-888

Project Staff
Vijay Divi and Professor Gregory Wornell

While traditionally a single sampling channel is used to capture an input, the use of multiple

channels to distribute the sampling load can help increase the system rate and resolution in a power efficient manner. Performance degrades in these systems due to timing-skew and other mismatch parameters; thus calibration is necessary. We develop efficient methods for blind parameter estimation and for signal estimation. We also examine the extreme case of a highly redundant amount of sampling channels, developing both calibration methods and performance bounds.

5. Technologies for Streaming Media Delivery

Sponsors
HP/MIT Alliance
NSF Grant No. CCF-0515109

Project Staff
Ying-zong Huang, John Apostolopoulos and Professor Gregory W. Wornell

The central problems of this research is motivated by some of the most pressing problems faced by the designers of streaming media systems in today's applications. An important issue is the reliable delivery of time-sensitive content in the face of unpredictable losses in the network.

For the reliable delivery problem, a practical joint packet selection and FEC system was proposed previously. While the coding protection of such a system added significant benefits to improve end-to-end distortion performance, it also added potentially long coding delay. This work extended the system to account for playout deadlines via optimizing selection and coding parameters against a hard delay constraint. An interesting insight of the extension is the separation of the selection scope of packets from their coding scope, as only the latter is subject to delay considerations. This insight allows a better design than a purely block-based version of the original (delay-unaware) scheme.

6. Secret Key Generation Using Sources and Channels

Sponsors
NSF Grant No. CCF-0515109
MIT/HP Alliance

Project Staff
Ashish Khisti and Professor Gregory Wornell

We study the problem of secret key generation between using information theoretic ideas of source and channel coding. The sender and receiver have access to a pair of correlated sources and communicate over a noisy channel. This secret key can then be used in a variety of cryptographic protocols.

In practice remote terminals can have access to correlated sources using a variety of techniques e.g., biometrics, satelite broadcast, channel reciprocity. The goal is to exploit these resources in conjunction with the underlying channel to develop novel techniques for key distillation.

7. Secure Transmission with Multiple Antennas

Sponsors
NSF Grant No. CCF 0515109

Project Staff
Ashish Khisti and Professor Gregory Wornell

Multiple-element antenna arrays are finding growing use in wireless communication networks. Much research to date has focused on the role of such arrays in enhancing the throughput and robustness for wireless communication systems. By contrast, this project focuses on the role of such arrays in a less explored aspect of wireless systems---enhancing security. Specifically, we develop and optimize physical layer techniques for using multiple antennas to protect digital transmissions from potential eavesdroppers, and analyze the resulting performance characteristics. Among the main results, we characterize the secrecy capacity of the multi-antenna-wiretap channel and develop several low complexity techniques to realize these gains for practical models.

8. Source Coding with Mismatched Distortion Measures

Sponsors
NSF Grant No. CCF-0515109

Project Staff
Urs Niesen, Assistant Professor Devavrat Shah and Professor Gregory W. Wornell

We consider the problem of lossy source coding with a mismatched distortion measure. That is, we investigate what distortion guarantees can be made with respect to distortion measure \tilde{\rho}, for a source code designed such that it achieves distortion less than D with respect to distortion measure \rho. We find a single-letter characterization of this mismatch distortion and study properties of this quantity. These results give insight into the robustness of lossy source coding with respect to modeling errors in the distortion measure. They also provide guidelines on how to choose a good tractable approximation of an intractable distortion measure.

9. Rateless Codes for MIMO Channels

Sponsors
NSERC
NSF Grant No. CCF-05151122
University IR&D Grant from Draper Laboratory
DoD MURI N00014-07-1-0738

Project Staff
Maryam Modir Shanechi, Professor Gregory W. Wornell and Professor Uri Erez

The design of practical and efficient codes for communicating over MIMO Gaussian channels when channel state information is not available a priori at the transmitter (or equivalently in a broadcast scenario where there are multiple receivers) is of significant interest in a variety of emerging wireless applications and standards. These include multiantenna systems as well as orthogonal frequency-division multiplexing (OFDM) systems.

For such problems, a rateless approach is rather natural, whereby an encoder maps a message into an infinite-length codeword for transmission over the channel. The decoder attempts to decode from successive prefixes of its received sequence. When it succeeds, it sends a single-bit

acknowledgment (ACK) to the encoder to terminate the transmission. As such, rateless codes are instances of hybrid ARQ (HARQ) Protocols.

In this work, we develop efficient hybrid ARQ protocols, i.e., rateless codes that achieve rates close to capacity and require low decoding complexity, for the MIMO Gaussian channel. The two time-invariant rateless code constructions developed employ layering, dithering, and repetition as key ingredients, and convert the MIMO channel into a scalar channel to which classical Gaussian base codes can be applied. Both constructions are convolutionally structured—one is based on faster-than-Nyquist (ftN) signaling, while the other on a diagonal layering (DL) structure. Moreover, both employ successive cancellation decoding. We show that ftN rateless codes are asymptotically capacity achieving at any signal-to-noise ratio (SNR) and induce a time-invariant scalar channel. We also show that DL codes are capacity achieving at any SNR, and induce a particular time-varying scalar channel to which standard LDPC base codes can be applied without significantly sacrificing performance.

10. Efficient Scheduling and Quantization for MIMO Broadcasting Systems with Limited Feedback

Sponsors
NSF Grant No. CCF-0635191
MITRE Corporation

Project Staff
Charles Swannack and Professor Gregory W. Wornell

There is growing interest in the development of efficient wireless broadcast systems for distributing independent data streams to different users over some geographical area. It is now widely appreciated that the use of a multiple-element antenna array at the transmitter can, in principle, greatly increase the capacity of such systems. When the number of users is no larger than the array size, the system design issues are rather well-understood. Moreover, when it is desirable for complexity or other reasons to restrict ones attention to case of linear multiplexing, the literature characterizing the associated performance tradeoffs is particularly extensive.

By contrast, comparatively little is known about how to design efficient systems when the number of users becomes large relative to the array size, and in particular the nature of the fundamental tradeoffs between throughput, complexity,and feedback in such settings. Ultimately, the underlying scheduling problem is rather different and in many ways richer than that of more traditional networks.

We develop and analyze a simple, low-complexity system architecture for scheduling over a Gaussian multiple-input multiple-output (MIMO) broadcast channel with infinite message backlogs. In the system of interest, there is a transmitter withm antennas, and n receiving users, where n x m. In a MIMO channel with choice over users, one expects to improve a particular performance criterion as a larger and larger user pool is searched. This could be maximizing total throughput (or sum rate),for example. The complexity of such an optimization is dominated by the underlying search for the best user subset to multiplex across the transmitter array, which must be performed each time an arriving packet or channel variation changes the system state. To reduce this complexity, one may limit the search to a smaller pool of users while ensuring that a set of users can be found in this restricted pool that obtains a sum rate which is close to optimal with high probability. We show that this proposed architecture is strongly asymptotically optimal with respect to average throughput. We further characterize the feedback requirements of the architecture, and highlight various tradeoffs available to the system designer.

This work further investigates the key aspects of joint scheduler-multiplexer design problem for multi-input multi-output (MIMO) systems, focusing on the problem of maximizing throughput

subject to complexity and limited feedback constraints when the number of users is a small multiple of the number of antennas. The problem of maximizing throughput in the multiuser MIMO broadcast channel is one of combining scheduling and spatial multiplexing (i.e., channel precoding). This has high algorithmic complexity in the number of users and transmit dimension, and for purposes of implementability it is of interest to find lower-complexity solutions.

11. Tracking Stopping Times Through Noisy Observations

Sponsors
NSF under Grant No. CCF-0515122
DoD MURI Grant No. N00014-07-1-0738
University R&D Grant from Draper Laboratory

Project Staff
Urs Niesen, Professor Gregory W. Wornell and Aslan Tchamkerten

We consider a generalization of the change-point problem, a well-known quickest detection problem in quality control. This generalization leads to interesting applications in prediction, monitoring, and communication.

Let $\{(X_i,Y_i)\}_{i\geq 1}$ be a sequence of pairs of random variables, and let S be a stopping time with respect to $\{(X_i,Y_i)\}_{i\geq 1}$. We consider the problem of finding a stopping time T with respect to $\{Y_i\}_{i\geq 1}$that optimally tracks S, in the sense that T minimizes the average reaction time $E(T-S)^+$, while keeps the false-alarm probability $P(T<S)$ below a given threshold $\alpha \in [0,1]$.

Here the (X_i,Y_i)'s take values in the same finite alphabet and S in bounded. By using elementary methods based on the analysis of the tree structure of stopping times, we first exhibit an algorithm that computes the optimal expected reaction times for all $\alpha \in [0,1]$ and constructs the associated optimal stopping times T. Second, we provide a sufficient condition on $\{(X_i,Y_i)\}_{i\geq 1}$and S under which the algorithm running time is polynomial in the bound of S. Finally we illustrate this condition with two examples: a Bayesian change-point problem and a pure tracking stopping time problem.

12. Secure Broadcasting over Fading Channels

Sponsors
NSF under Grant No. CCF-0515122
University R&D Grant from Draper Laboratory

Project Staff
Ashish Khisti, Professory Gregory Wornell, and Aslan Tchamkerten

Wyner's wiretap channel is extended to parallel broadcast channels and fading channels with multiple receivers. In the first part of the paper, we consider the setup of parallel broadcast channels with one sender, multiple intended receivers, and one eavesdropper. We study the situations where the sender broadcasts either a common message or independent messages to the intended receivers. We derive upper and lower bounds on the common-message-secrecy capacity, which coincide when the users are reversely degraded. For the case of independent messages we establish the secrecy sum-capacity when the users are reversely degraded.

In the second part of the paper we apply our results to fading channels: perfect channel state

information of all intended receivers is known globally, whereas the eavesdropper channel is known only to her. For the common message case, a somewhat surprising result is proven: a positive rate can be achieved independently of the number of intended receivers. For independent messages, an opportunistic transmission scheme is presented that achieves the secrecy sum-capacity in the limit of large number of receivers. Our results are stated for a fast fading channel model. Extensions to the block fading model are also discussed.

13. Asynchronous Communication

Sponsors
NSF Grant No. CCF-0515122
DoD MURI Grant No. N00014-07-1-0738
University IR&D Grant from Draper Laboratory

Project Staff
Venkat Chandar, Professor Gregory Wornell and Aslan Tchamkerten

It seems fair to say that in information theory the assumption of perfect synchronized communicating parties is ubiquitous and that the theory gives little insight on how to handle issues related to time uncertainty.

The basic question we address here is `how does a lack of synchronization between the transmitter and the receiver affect the range of achievable communication rates?'. To that aim we introduce a discrete time asynchronous channel model for point-to-point communication that can be seen as an extension of the detection and isolation problem setting in sequential analysis: the transmitter may start emitting information at any time within a certain interval that represents the level of asynchronism. The receiver must decode without knowing when transmission starts but being cognizant of the asynchronism level. Our main result is the characterization of the largest asynchronism level for which reliable communication can be achieved. Specifically we show that, among all coding schemes that operate at a strictly positive rate, the maximum achievable asynchronism level is (asymptotically) $e^{\alpha N}$ where N denotes the codeword length and where α represents the `synchronization threshold' and admits a simple expression depending on the channel. The scheme we propose to reliably communicate under strong asynchronism, perhaps somewhat surprisingly, performs detection of the codeword and isolation of the message jointly rather than separately as often in practice.

14. RFID Authenication Protocol Secure Against Relay Attacks

Sponsors
NSF Grant No. CCF-0515122
University IR&D Grant from Draper Laboratory

Project Staff
Gildas Avoine and Aslan Tchamkerten

Relay attacks are a major concern for RFID systems: during an authentication process an adversary transparently relays messages between a verifier and a remote legitimate prover. We present an authentication protocol suited for RFID systems. Our solution is the first that prevents relay attacks without degrading the authentication security level: it minimizes the probability that the verifier accepts a fake proof of identity, whether or not a relay attack occurs. Of practical interest, our protocol enables the verifier to make a rational decision to accept or to reject a partial proof of identity— say, caused by an unexpected protocol interruption.

Publications

Journal Articles, Published

L. Brooks and H-S. Lee, “A Zero-Crossing Based 200MS/s 8b Pipelined ADC,” *IEEE Journal of Solid State Circuits,* 42: 2677–2687 (2007).

Journal Articles, Accepted for Publication

L. Brooks and H.S. Lee, “Background Calibration of Pipelined ADCs Via Decision Boundary Gap Estimation,” *IEEE Transactions on Circuits and Systems- I,* forthcoming.

V. Chandar, A. Tchamkerten, and G. W. Wornell, “Optimal Sequential Frame Synchronization,” *IEEE Transactions on Information Theory*, forthcoming August 2008.

E. Martinian, G. W. Wornell, and R. Zamir, “Source Coding with Distortion Side Information,” to appear *IEEE Trans. Inform. Theory*, forthcoming October 2008.

A. Tchamkerten, V. Chandar, G. W. Wornell, "Communication under Strong Asynchronism," to appear in *IEEE Trans. Info. Theory*

Journal Articles, Submitted for Publication

U. Erez, M. D. Trott, and G. W. Wornell, “Rateless Coding for Gaussian Channels,” submitted to *IEEE Transactions on Information Theory*.

A. Khisti and G. W. Wornell, “Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel,” submitted to *IEEE Transactions on Information Theory*.

U. Niesen, D. Shah, G. W. Wornell, “Source coding with Mismatched Distortion Measures,” submitted to *IEEE Transactions on Information Theory*.

U. Niesen, A. Tchamkerten, and G. W. Wornell, “Tracking Stopping Times Through Noisy Observations,” submitted to *IEEE Transactions on Information Theory*.

Meeting Papers, Published

V. Divi and G. W. Wornell, “Bandlimited Signal Reconstruction from Noisy Periodic Nonuniform Samples in Time-interleaved ADCs,” *Proceedings of IEEE ICASSP, (*Las Vegas), March/April 2008.

U. Erez, M.D. Trott, and G. W. Wornell, “An Efficient ARQ Scheme with SNR Feedback,” in *Proc. Int. Zurich Seminar Commun.,* (Zurich, Switzerland), March 2008.

E. W. Huang and G. W. Wornell, “Peak to Average Power Reduction for Low-Power OFDM Systems,” in *Proc. Int. Commun. Conference* (Glasgow, Scotland), June 2007.

A. Khisti and G. W. Wornell, “The MIMOME Channel,” in *Proceedings of Allerton Conference Communication Control and Computing*, (Illinois), September 2007.

A. Khisti, G. W. Wornell, A. Wiesel, and Y. Edlar, “On the Gaussian MIMO Wiretap Channel,” in *Proc. Int. Symp. Inform. Theory*, (ISIT) (Toronto, Canada), June 2007.

U. Niesen, D. Shah, and G. W. Wornell, “ Source Coding with Mismatched Distortion Measures,” *Proceedings of Allerton Conference Communication Control and Computing*, (Illinois), September 2007.

U. Niesen, D. Shah, and G. W. Wornell, “Adaptive Alternating Minimization Algorithms,” in *Proc. Int. Symp. Inform. Theory*, (ISIT) (Toronto, Canada), June 2007.

U. Niesen, A. Tchamkerten, and G. W. Wornell, “The Complexity of Tracking a Stopping Time,” *Proc. IEEE International Symposium on Information Theory (ISIT*), June 2007.

J. M. Shapiro, R. J. Barron, and G. W. Wornell,” Practical Layered Rateless Codes for the Gaussian Channel: Power Allocation and Implementation,” in *Proc. IEEE Workshop Signal Processing Adv., Wireless Commun.* (SPAWC-2007), (Helsinki, Finland), June 2007.

M. Shanechi, U. Erez, and G. W. Wornell, “On Universal Coding for Parallel Gaussian Channels,” in *Proc. Int. Zurich Seminar Communication*, (Zurich, Switzerland), March 2008.

A. Tchamkerten, V. Chandar, G. W. Wornell, “On the Capacity Region of Asynchronous Channels,” in *Proc. Int. Symp. on Inform. Theory (ISIT*), June 2007.

A. Tchamkerten, V. Chandar, and G. W. Wornell, “Frame Ailgnment and Communication under Strong Asynchronism,” *Proceedings of Allerton Conference Communication Control and Computing*, (Illinois), September 2007.

Theses

L. Brooks, *Circuits and Algorithms for Pipelined ADCs in Scaled CMOS Technologies,* Ph.D. diss., Department of Electrical Engineering and Computer Science, MIT, 2008.