RESEARCH REPORT
Telecom: Circuits, Devices, & Systems
Integrated circuits, low-power wireless sensors, semiconductors, signal processing, broadband, algorithmic, fault diagnosis, optical networks, network architecture, power analysis, self-powered electronic systems
Telecommunications: Circuits, Devices, and Systems

This report by MIT's Industrial Liaison Program identifies MIT research in the area of circuits, devices and systems within telecommunications.

For more information, please contact MIT's Industrial Liaison Program at +1-617-253-2691.

### DEPARTMENTS, GROUPS AND LABORATORIES

<table>
<thead>
<tr>
<th>Department/Group/Program</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Telecommunications and Signal Processing Group</td>
<td>5</td>
</tr>
<tr>
<td>Center for Integrated Circuits and Systems (CICS)</td>
<td>5</td>
</tr>
<tr>
<td>Digital Integrated Circuits and Systems Group</td>
<td>6</td>
</tr>
<tr>
<td>Laboratory for Electromagnetic and Electronic Systems (LEES)</td>
<td>6</td>
</tr>
<tr>
<td>Laboratory for Information and Decision Systems (LIDS)</td>
<td>6</td>
</tr>
<tr>
<td>Microsystems Technology Laboratories (MTL)</td>
<td>7</td>
</tr>
<tr>
<td>Nokia Research Center Cambridge</td>
<td>7</td>
</tr>
<tr>
<td>Remote Sensing and Estimation Group (RSEG)</td>
<td>7</td>
</tr>
<tr>
<td>Research Laboratory of Electronics (RLE)</td>
<td>8</td>
</tr>
<tr>
<td>Signals, Information, and Algorithms Laboratory</td>
<td>8</td>
</tr>
</tbody>
</table>

### FACULTY RESEARCH PROJECTS

<table>
<thead>
<tr>
<th>Professor</th>
<th>Project Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROF. ARVIND</td>
<td>ARMO: Synthesizable Modeling of Mobile Phones to Facilitate Architectural Studies of Performance and Energy-Efficiency</td>
</tr>
<tr>
<td>PROF. VINCENT W S CHAN</td>
<td>From WiFi to WiMAX: Techniques for IP Reuse Across Different OFDM Protocols</td>
</tr>
<tr>
<td>PROF. ARVIND</td>
<td>Adaptive Fault Diagnosis Schemes</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Cost-Effective Fault Diagnosis for All-Optical Networks</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Cost-Efficient Physical Architecture for OXC-Switched WDM Mesh Networks</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Development of Two Network Topology Management Algorithms</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Feasibility Study of the Proposed Network Architecture</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Future Optical Network Architectures</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Impact of Signal Processing Energy and Large Bandwidth on Infrastructureless Wireless Network Routing and Scalability</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Non-Adaptive Fault Diagnosis Schemes</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Performance-Cost Tradeoffs of Optical Transport Architectures</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Proactive Wireless Networks</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Quantification of Network Gains</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Claude E Shannon Communication and Network Group (CNG)</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>Satellite Networks and Architectures</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>A High-Density 45-nm SRAM Using Small-Signal Non-Strobed Regenerative Sensing</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>SRAM Design for Ultra-Low-Power Systems</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>A Highly Digital, Resolution- and Voltage-Scalable SAR ADC</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>An AES-Based Energy-Efficient Encryption Processor with Resistance to Differential Power Analysis Attacks</td>
</tr>
<tr>
<td>PROF. ANANTHA P. CHANDRAKASAN</td>
<td>On-Chip Voltage-Scalable Switched-capacitor DC-DC Converter</td>
</tr>
</tbody>
</table>
Self-Powered Electronic Systems ................................................................. 24
A 65-nm, Sub-V(t) Microcontroller with Integrated SRAM and DC-DC Converter ................................................................. 24
Algorithms and Architectures for Ultra-low-power Video Compression ................................................................. 25
An Ultra-Low Power CMOS RF Transceiver for Medical Implants ................................................................. 25
Design and Characterization of CNT-CMOS Hybrid Systems ................................................................. 26
Minimum Energy Tracking Loop with Embedded DC-DC Converter in 65-nm CMOS ................................................................. 26
Reaching the Optimal Mixed-Signal Energy Point ................................................................. 27
Reconfigurable Zero-Crossing-Based Analog Circuits ................................................................. 28

PROF. HAE-SEUNG LEE ........................................................................ 28
Comparator-Based Circuits for HBTs ................................................................. 28
A Zero-Crossing Based, 8b, 200MS/s Pipelined ADC ................................................................. 29
High-Accuracy Pipelined A/D Converter Based on Zero-Crossing Switched Capacitor Circuits ................................................................. 30
Ultra-High Speed A/D Converters Using Zero-Crossing-Based Circuits ................................................................. 30

PROF. JAE S. LIM ........................................................................ 31
Advanced Telecommunications and Signal Processing (ATS) Group ................................................................. 31
Transforms for Prediction Residuals in Video Coding ................................................................. 32
Transforms for Prediction Residuals in Multiview Video Coding ................................................................. 33
Improvement of H.264 Using JPEG 2000 Technology ................................................................. 34
Image Fusion: Increase of Depth-of-Field by Combination of Multiple Images ................................................................. 35

PROF. SETH LLOYD ........................................................................ 36
Keck Foundation Center for Extreme Quantum Information Theory (xQIT) ................................................................. 36
Quantum Communication ................................................................. 37
xQIT: The Pressing Need for Advances in Extreme Quantum Infomation Theory ................................................................. 37
xQIT: Fundamental Limits on Quantum Sensing and Control ................................................................. 38

PROF. MURIEL MEDARD ........................................................................ 39
Optical Networks ................................................................. 39
Evolutionary Methods in Network Coding Applied to MANETs ................................................................. 39
Information Theory for MANETs ................................................................. 41
Information-Theoretic Aspects of Network Coding ................................................................. 42
Joint Source and Network Coding ................................................................. 43
Practical Approaches to Wireless Network Coding ................................................................. 43
Security Aspects of Network Coding ................................................................. 45

DR. UNA-MAY O’REILLY ........................................................................ 47
Evolutionary Design and Optimization Group (EVO-DesignOpt) ................................................................. 47
Genetic Algorithms for Network Coding ................................................................. 48
An Evolutionary Approach to Network Coding Problems ................................................................. 48

PROF. JEFFREY H SHAPIRO ........................................................................ 49
Quantum Information Technology: Entanglement, Teleportation and Quantum Memory ................................................................. 49
xQIT: Capacities and Coding for Quantum Communication Channels ................................................................. 51

PROF. CHARLES G. SODINI ........................................................................ 51
Coding in Wideband OFDM Wireless Communications with Adaptive Modulation ................................................................. 51
Power Amplifier Design for Millimeter-Wave Imaging ................................................................. 52

PROF. JOHN R WILLIAMS ........................................................................ 53
The Internet of Things ................................................................. 53

PROF. MOE Z. WIN ........................................................................ 53
Wireless Communication and Network Sciences Laboratory ................................................................. 53
Cooperative and Distributed Techniques ................................................................. 54
Cooperative Localization for UWB Networks ................................................................. 54
Interference Analysis in Heterogeneous Network ................................................................. 55
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimal Search Strategies</td>
<td>55</td>
</tr>
<tr>
<td>Quantum Error Recovery</td>
<td>56</td>
</tr>
<tr>
<td>Subset Diversity Techniques</td>
<td>56</td>
</tr>
<tr>
<td>Ultra-Wide Bandwidth (UWB) Communications</td>
<td>57</td>
</tr>
<tr>
<td>PROF. GREGORY W. WORNELL</td>
<td>57</td>
</tr>
<tr>
<td>Circuits and Algorithms for Pipelined ADCs in Scaled CMOS Technology</td>
<td>57</td>
</tr>
<tr>
<td>Digital Processing in Imaging Systems</td>
<td>58</td>
</tr>
<tr>
<td>Secret Key Generation Using Sources and Channels</td>
<td>58</td>
</tr>
<tr>
<td>Secure Broadcasting Over Fading Channels</td>
<td>58</td>
</tr>
<tr>
<td>Technologies for Streaming Media Delivery</td>
<td>59</td>
</tr>
<tr>
<td>The Impact of Asynchronism on Communication</td>
<td>59</td>
</tr>
<tr>
<td>Multimedia Compression with Encoder Side Information</td>
<td>59</td>
</tr>
<tr>
<td>Ultralow-Complexity Iterative Interference Cancellation</td>
<td>60</td>
</tr>
<tr>
<td>Asynchronous Communication</td>
<td>60</td>
</tr>
<tr>
<td>Secure Transmission with Multiple Antennas</td>
<td>60</td>
</tr>
<tr>
<td>Hewlett-Packard Wireless Invent@MIT</td>
<td>61</td>
</tr>
<tr>
<td>Efficient Scheduling and Quantization for MIMO Broadcasting Systems</td>
<td>61</td>
</tr>
<tr>
<td>Information Theoretic Perspectives on Synchronization</td>
<td>61</td>
</tr>
</tbody>
</table>
DEPARTMENTS, GROUPS AND LABORATORIES

ADVANCED TELECOMMUNICATIONS AND SIGNAL PROCESSING GROUP
Principal Investigator: Jae S Lim

The present television system was designed nearly 60 years ago. Since then, there have been significant developments in technology, which are highly relevant to the television industries. For example, advances in the very large scale integration (VLSI) technology and signal processing theories make it feasible to incorporate frame-store memory and sophisticated signal processing capabilities in a television receiver at a reasonable cost. To exploit this new technology in developing future television systems, the research areas of the program focused on a number of issues related to digital television design. As a result of this effort, significant advances have already been made and these advances have been included in the U.S. digital television standard. Specifically, the ATSP group represented MIT in MIT's participation in the Grand Alliance, which consisted of MIT, AT&T, Zenith Electronics Corporation, General Instrument Corporation, David Sarnoff Research Center, Philips Laboratories, and Thomson Consumer Electronics. The Grand Alliance digital television system served as the basis for the U.S. Digital Television (DTV) standard, which was formally adopted by the U.S. Federal Communications Commission in December 1996.

The digital TV system based on this standard has been deployed successfully. In 2006, digital television receiver sales exceeded analog television receivers in both number and dollar volume in the U.S. The analog terrestrial TV transmission was discontinued in the U.S. in June 2009.

The standard imposes substantial constraints on the way the digital television signal is transmitted and received. The standard also leaves considerable room for future improvements through technological advances. Current research focuses on making these future improvements. In addition to research on issues related to the design of digital television system, the research program also includes research on signal processing for telecommunications applications.

CENTER FOR INTEGRATED CIRCUITS AND SYSTEMS (CICS)
Principal Investigator: Hae-Seung Lee
http://mtlweb.mit.edu/researchgroups/cics/

The Research Center for Integrated Circuits and Systems (CICS) is a form of an industrial consortium created to promote new research initiatives in circuits and systems design, as well as to promote tighter technical relation between MIT's research and relevant industry. The group has been investigating a wide range of circuits and systems related to wireless communication, microsensor/actuator systems, imagers, digital and analog signal processing circuits, dc-dc converters, and many other systems.

The Center for Integrated Circuits and Systems (CICS) serves to promote closer technical relation between MIT's Microsystems Technology Lab's (MTL) research and industry, initiate and fund new research in integrated circuits and systems, produce more students skilled in the same area,
address important research issues relevant to industry, and solicit ideas for new research from industry.

**DIGITAL INTEGRATED CIRCUITS AND SYSTEMS GROUP**
Principal Investigator: Ananth Chandrakasan
http://mtlweb.mit.edu/researchgroups/icsystems/index.html

The Digital Integrated Circuits and Systems Group is involved with the design and implementation of various integrated systems ranging from ultra low-power wireless sensors and multimedia devices to high-performance processors. The research spans across multiple levels of abstraction ranging from innovative new process technologies and circuit styles to architectures, algorithms, and software technologies. A key focus of this group is developing energy-efficient integrated solutions for battery-operated systems.

**The UWB Project:** As an alternative to traditional narrowband data transmission, UWB offers a drastically new framework in which frequency concepts are replaced by time domain concepts and transient analysis appears naturally. This system offers high data-rates, low interference and allows an almost completely digital implementation.

**The Sub-Threshold Circuits Group:** The MIT Sub-Threshold Circuits Group explores energy-efficient techniques that take advantage of sub-threshold operation. The group’s work span different levels of abstraction, from analyzing the optimal energy point of a given system, modeling energy characteristics of sub-threshold circuits, to developing circuit styles for logic and memory elements that operate at ultra-low voltages.

**LABORATORY FOR ELECTROMAGNETIC AND ELECTRONIC SYSTEMS (LEES)**
Principal Investigator: John G Kassakian
http://lees.mit.edu/lees/

The Laboratory for Electromagnetic and Electronic Systems (LEES) provides the theoretical basis, and component, circuit and system technologies required to develop advanced electrical energy applications. LEES research areas include electronic circuits, components and systems, power electronics and control, micro and macro electromechanics, electromagnetics, continuum mechanics (the interaction of fields with fluids and other deformable media), high voltage engineering and dielectric physics, manufacturing and process control, and energy economics.

**LABORATORY FOR INFORMATION AND DECISION SYSTEMS (LIDS)**
Principal Investigator: Alan S Willsky
http://lids.mit.edu/

The Laboratory for Information and Decision Systems (LIDS) is an interdepartmental research laboratory at the Massachusetts Institute of Technology. LIDS’ fundamental research goal is to advance the field of systems, communications and control. In doing this, it recognizes the interdependence of these fields and the fundamental role that computation plays in this research. The Laboratory conducts basic theoretical studies in communication and control and is committed to advancing the state of knowledge of technologically important areas such as atmospheric optical communications and multivariable robust control.
Its staff includes faculty members, full-time research scientists, postdoctoral fellows, graduate research assistants, and support personnel. Undergraduate students participate in the research program of the Laboratory through the Undergraduate Research Opportunities Program (UROP). Every year several research scientists from various parts of the world visit the Laboratory to participate in its research program.

MICROSYSTEMS TECHNOLOGY LABORATORIES (MTL)
Principal Investigator: Anantha P Chandrakasan
http://mtlweb.mit.edu/

The Microsystems Technology Laboratories (MTL) at MIT is an interdepartmental laboratory supporting research and education in micro- and nano- systems. MTL was established in the mid-1980s inside the Electrical Engineering and Computer Science Department. Over the years, MTL has evolved and grown into an Interdepartmental laboratory reporting to the Dean of the School of Engineering, reaching across the entire Institute. MTL is an Interdepartmental Laboratory that encompasses research and education with an intellectual core of:

- Semiconductor Process and Device Technology
- Integrated Circuits and Systems Design
- MTL fosters new initiatives in Microsystems at the Institute
- MTL provides Microsystems infrastructure to research groups across the Institute

NOKIA RESEARCH CENTER CAMBRIDGE
http://projects.csail.mit.edu/nrcc/projects.php

NRCC (Nokia Research Center Cambridge) is a cross-disciplinary research organization whose charter is to bring new ideas into Nokia products. NRCC consists of approximately 20 Nokia researchers, investigating all aspects of mobile phones, from computer and network architecture to user interfaces. The primary activity of Nokia Research Center Cambridge is the Nokia-MIT Collaboration. The Nokia-MIT Collaboration builds on past cooperation with MIT, including W3C, Project Oxygen, Things That Think, and the Communications Futures Program. One of the goals of the collaboration is to increase the level of interaction between Nokia and MIT researchers compared to previous initiatives. For this reason, NRCC has been situated close to MIT CSAIL with spare offices for external researchers.

REMOTE SENSING AND ESTIMATION GROUP (RSEG)
Principal Investigator: David H Staelin
http://rseg.mit.edu/

RSEG is actively engaged in research on 1) improved methods for estimating unknown parameters from multivariate data, particularly from generic blind data, data obtained by passive multi-spectral imaging remote sensing satellites, and wireless communications, 2) advancing the state-of-the-art of passive microwave and infrared remote sensing of the atmosphere from aircraft and spacecraft, particularly for purposes of sounding atmospheric temperature, humidity, and precipitation profiles, 3) use of satellite data to characterize the earth, and particularly its global precipitation, and 4) development of self-organizing RF spectrum allocation techniques for
Internet and other applications. The remote sensing work also includes development and
operation of passive microwave spectral imagers at millimeter and sub-millimeter wavelengths,
and development of the associated calibration techniques for aircraft and spacecraft. The wireless
communications program includes development and utilization of multiport sensors for
characterizing wireless propagation and spectrum use. Prior and related work has also involved
video image processing, optical astrometric interferometers, multi-mode controlled structures,
design of experiments, manufacturing process characterization and optimization, pulsar radio
astronomy, planetary radio astronomy, communications network architecture, and other topics.

**RESEARCH LABORATORY OF ELECTRONICS (RLE)**
Principal Investigator: Jeffrey H Shapiro
http://www.rle.mit.edu/

The RLE is home to a wide range of sponsored research activities centered in four broad areas:
electronics, optics, and photonics; communications and signal processing; atomic, molecular, and
optical physics; and "living systems," particularly language, speech, hearing, and haptics. RLE
research activities are both basic and applied, occupying the rich area spanning fundamental
research and the development of contemporary technology. Recently, important new initiatives
have been launched to investigate the physics of ultracold atoms and to explore quantum
information technology and computing. RLE faculty and staff come from various academic
departments at MIT, primarily the Department of Electrical Engineering and Computer Science
and the Department of Physics, but also from the Departments of Mechanical Engineering and
Materials Science and Engineering. RLE comprises fifty-four principal investigators and a total of
approximately 500 faculty, students, and staff.

**SIGNALS, INFORMATION, AND ALGORITHMS LABORATORY**
Principal Investigator: Gregory W Wornell
http://www.rle.mit.edu/sia/

The lab's focus is on developing efficient algorithmic structures to address emerging problems of
fundamental interest involving the manipulation of signals and information in diverse settings.
The lab's research ranges from the development of fundamental limits and architectural
principles, to implementation issues and experimental investigations. Of particular emphasis in
recent years have been problems arising in the context of wireless, sensor, multimedia, and
broadband networks.

Some of the topics of 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
FACULTY RESEARCH PROJECTS

PROF. ARVIND
Charles W and Jennifer C Johnson Professor of Electrical Engineering and Computer Science
Head, Computation Structures Group (CSAIL)
Program Manager, Nokia Research Center Cambridge
http://csg.csail.mit.edu/Users/arvind/

Arvind’s current research interests are synthesis and verification of large digital systems described using Guarded Atomic Actions; and Memory Models and Cache Coherence Protocols for parallel architectures and languages. In the past, Arvind's research interests have included all aspects of parallel computing and declarative programming languages. He has contributed to the development of dynamic dataflow architectures, the implicitly parallel programming languages Id and pH, and the compilation of these types of languages on parallel machines. Dr. R. S. Nikhil and Arvind published the book "Implicit parallel programming in pH" in 2001.

ARMO: Synthesizable Modeling of Mobile Phones to Facilitate Architectural Studies of Performance and Energy-Efficiency

There is an increasing need to support a variety of applications on mobile phones, and many will be developed by Independent Software Vendors. This need is transforming the perception of a mobile phone from an embedded device into a stable platform for software development. Nevertheless, Mobile phones will continue to have an "embedded device" character because the device must be small, dissipate less than 3 watts maximum, and be able to operate for days on battery power. This dual characteristic of a mobile phone as a platform and as an embedded device provides many research challenges. Because of the stringent performance and power requirements, a mobile system might be implemented with a mixture of hardware and software components, and software components could be partitioned across multiple parallel general-purpose processors or DSPs. The appropriate implementation of a component could even change from hardware to software depending on performance and power requirements. Perhaps the right way to think about designing a mobile platform will not be as a general-purpose processor programmed using serial languages and libraries of APIs, but rather as a collection of concurrently executing modules which support the right level of functionality for a given market.

ARMO stands for ARchitecture MOdeling (in Finnish it means Grace!). The principal underlying technology in this project is a modular system implementation methodology based on Guarded Atomic Actions and Decoupled Systems. This methodology allows a single module specification to be automatically translated into high-quality hardware implementations or high-quality software implementations, with automatic generation of interfaces between the domains. This vision will enable a complete mobile phone to be "assembled" rapidly from existing or new modules, where each module is mapped to either hardware or software according to performance and power requirements. We will show via example implementations that a design methodology based on Guarded Atomic Actions and Decoupled Systems allows packaging of Intellectual Property in a way that is highly reusable because of parameterization and flexible interfaces. We expect our design flow to dramatically reduce the design cost and risk for implementing custom hardware blocks that interact seamlessly with software modules. An important component of this project is to quantify the performance and power consumption of different implementation technologies used to implement computationally intensive functions required in a mobile terminal.
To support all of these efforts, we will build a full-system modeling framework, where different components can be simulated at different levels of abstraction (functional, transactional, cycle-level). This may also result in a non-proprietary model of a mobile phone that can be shared with other academic and outside researchers. Within this proposal, the full system model will be used to explore new capabilities in mobile platform architecture, including hardware security mechanisms and high-bandwidth wireless links.

**From WiFi to WiMAX: Techniques for IP Reuse Across Different OFDM Protocols**

Since the early 1990's, there has been a rapid evolution in digital wireless protocols to enable higher data rates, improve bandwidth efficiency and offer services to more users. There is a dramatic shift from purely voice based services to high bit-rate data services to support web browsing, VoIP and high definition video. The underlying technology that enables this high data rate in non-line-of-sight environment is a modulation scheme known as Orthogonal Frequency Division Multiplexing (OFDM). OFDM has been around for several decades, but its robustness to multipath interference has been proven in practice by widespread deployment of 802.11a/g and ADSL. Since then, OFDM has become the most preferred modulation scheme for both broadband and high bit-rate digital wireless protocols.

Although the components and overall structure of different OFDM protocols are functionally similar, the characteristics of the environment for which a wireless protocol is designed often result in different instantiations of various components with different algorithmic settings. It is in general difficult to develop IP blocks that can be reused across different protocols because the IP blocks developed are either not flexible enough to support the required algorithmic settings or they have unnecessary logics to support unused algorithmic settings.

We demonstrate that it is possible to generate efficient hardware for two different wireless protocols, namely 802.11a and 802.16, from the same code base written in Bluespec SystemVerilog (BSV). The following two features are essential for such designs: 1) a polymorphic type system that permits highly parameterized codes and 2) the ability to compose independently created modules with predictable functionality and performance. The latter capability permits the refinement of individual modules to meet the performance objectives and exploration of area-performance tradeoffs without exacerbating the verification problem. Bluespec provides the unique capability of synthesizing such designs into efficient hardware. Parameterization in Bluespec has no cost because it results in no extra logic -- all the static parameterization is automatically removed by the compiler during the static elaboration phase of the compilation.

We decompose a generic OFDM baseband transceiver into multiple well-defined blocks. We focus on implementing highly-parameterized base-band processing blocks from which we can derive different instances to support multiple radio protocols. In the approach, only the transmitter and receiver controllers are protocol specific and non-reusable.

We employ several techniques to enable significant module reuse and customization across different protocols, architectures, and design points. The high-level structure in which modules are interconnected follows a transaction-level modeling style. Furthermore, we restrict communication between the modules to pass OFDM messages containing control and data values. The control part of the message is generated by the controller and is used to communicate to each module what is to be done with the data. The control part is not modified by any module as the message flows through the pipeline and is stripped off before the message leaves the base
band processing section. The control part varies in type and value for different protocols; a challenge in coding reusable modules is to relate different (dynamic) control information to the different (static) instantiations of a module. The solution to this problem is to ask the designer to pass a function parameter that explains how to extract the internal module control information from the external protocol specific control information when one instantiates a module.

We have implemented a library of parameterized blocks and used them to implement the transceivers of 802.11a and 802.16. With this approach, 4,028 lines of code are shared between the two transceivers which are over 90% of the total lines of code for each design.

We have obtained the synthesis results for the two transceivers with Synopsis Design Compiler with the TSMC 180nm library. We find that the code is synthesizable into high quality hardware.

In the future, we would like to evaluate if the library is rich enough to implement other ODFM protocols.

**PROF. VINCENT W S CHAN**

Joan and Irwin M Jacobs (1957) Professor of Electrical Engineering and Computer Science and Aeronautics and Astronautics  
http://web.mit.edu/chan/www/

Vincent Chan’s research focuses on optical fiber networks, where the challenge is providing orders of magnitude improvement in performance at an affordable cost, an important theme for industry, indicates Chan. With other LIDS faculty, Chan is working on new optical transport mechanisms to radically change the responsiveness and cost structure of high-speed networks. Other projects include a new all-optical transport mechanism with extreme agility and new diagnostic techniques that rapidly locate all optical network failures. Research on free space optical communications over the turbulent atmospheric channel has begun to investigate fading mitigation techniques.

Chan’s work in space communications is very new and still a step behind ground-based telecommunications. The future for the Internet is to use satellite and space links to provide service that mirrors that available on the ground. This poses significant challenges.

**Adaptive Fault Diagnosis Schemes**

In adaptive fault diagnosis schemes, probing signals are sequentially sent to probe the health of the network until the failure pattern is identified. Owing to its sequential nature, successive probes can be chosen according to previous probe syndromes, and thus the number of probes required is usually quite small. However, the number of probing steps might be quite large for some network failure patterns and/or in some large networks. Indeed, the design objective is to minimize the average number of probes to identify any failure pattern.

Under the probabilistic link failure model, we have established a mathematical mapping between the fault diagnosis problem in network management and the source coding problem in Information Theory, under the constraint that only probes along lightpaths in the network are permissible. This mapping has both theoretical and practical implications in designing efficient adaptive fault diagnosis schemes for all-optical networks.
With a deep understanding of the run-length probing scheme for Eulerian network with probabilistic link failures, we have extended its applications to more practical situations such as non-Eulerian networks with link failures and networks with link/node failures. For non-Eulerian networks with probabilistic link failures, we suggested two alternative approaches to deploy the run-length probing scheme: (1) the disjoint trail decomposition approach that decomposes the network into a set of link-disjoint trails for diagnosis, and (2) the path augmentation approach that replicates a minimum set of links to make the network Eulerian.

The analytical and numerical investigations reveal a guideline for efficient fault diagnosis schemes: each probe should provide approximately 1-bit of information and the total number of probes required is approximately equal to the entropy of the state of the network. This result provides an insightful guideline to reduce the overhead cost of fault management for all-optical networks and can further the understanding of the relationship between information entropy and network management.

**Cost-Effective Fault Diagnosis for All-Optical Networks**

All-optical networks, where data traverse lightpaths without any optical-to-electronic conversion at intermediate nodes, promise significant cost benefits. The significant cost savings are due to optical switching of high data-rate lightpaths at intermediate network nodes, thereby reducing electronic processing costs. As a result, broadband network services can potentially be delivered to large populations at much lower cost than today's technologies. However, without the electronic processing capability at intermediate nodes, network architects have to develop new technologies to address problems whose solutions previously rely on the electronic processing capability at intermediate nodes. In particular, all-optical networks are susceptible to various physical failures, e.g., fiber cuts, switch node failures, transmitter/receiver breakdowns, and optical amplifier breakdowns. These failures can result in the disruption of communication, and can be costly to detect and localize within the current management framework (e.g. SONET/G.709). Since all-optical networks lack parity checks at intermediate nodes as SONET/G.709 does, either optical signal is tapped out at each intermediate node for parity check or new mechanisms are needed to diagnose link/node failures. If tapping is indeed done, a lot of cost gains of all-optical networks will be mitigated. Therefore, we aim to develop new fault diagnosis approach to keep the network operating cost low.

Instead of the passive paradigm based on parity check in SONET/G.709, we have proposed a proactive fault diagnosis paradigm: optical probing signals are sent along some lightpaths to test the health of the network, and probe syndromes (i.e., results of the probes) are used to differentiate failure patterns. The design of proactive fault diagnosis schemes for all-optical networks bears two key objectives: (i) detecting faults quickly, and (ii) keeping the diagnosis cost low. The importance of objective (i) stems from the current SONET standard, in which the 50-ms restoration time leaves little room for fault detection and localization. This will probably be reduced further in future all-optical networks to avoid large amount of data loss during a short period of communication disruption. Hence, when parts of a network are malfunctioning, it is critical to locate and identify these failures as soon as possible. At the same time, the cost of fault diagnosis has to be kept low such that the cost advantage of all-optical networks, compared to traditional optical networks, can materialize.

We believe that the two design objectives could be tightly related to two parameters of proactive fault diagnosis schemes (i.e., the number of probes and the number of probing steps). First, the number of probes could serve as the manifestation of fault management effort. In particular, each
probe requires certain amount of effort in both network management/control plane (e.g., signaling) and data plane (e.g., transmission and detection) that otherwise could be used to generate revenue. In addition, each probe results in one bit of management information, whose transportation, storage and processing consumes additional network resources. Second, under the assumption that each step takes approximately equal amount of time, the number of probing steps indicates how fast the fault pattern could be identified. In this research, we exploit two alternative designs for choosing probes (i.e., adaptive probing, and non-adaptive probing) to balance these two objectives.

Cost-Efficient Physical Architecture for OXC-Switched WDM Mesh Networks

In current telecom environment, carriers have deployed huge capacity in the long-haul networks. At the meantime, end users' access to higher data rates is still costly. To bridge the gap between the bandwidth glut at the backbone and the high access cost for the end-users, the architecture of next generation optical MAN will be an important contributor to the reduction of access network cost. The objective is to design networks that not only require a low installation cost, but also have good scalability -- a decreasing cost-per-node-per-unit-traffic as the number of users and transaction size increase. This architecture feature is essential for any commercially deployed network to attract serious providers and investors to commit to the venture as part of a sensible business.

The central theme of this thesis is to identify scalable network architectures over the possibilities of optical networks as allowed by the technology: fiber connection topologies, switching technology selection and dimensioning, as well as routing and wavelengths assignment, with emphasis on exploring the benefit of optimizing over fiber connection topologies. Due to the intrinsic complexity of such an optimization problem and because of our interest in gaining insights into how the cost structures drive architectural tradeoffs, for the first part of this thesis, we take an analytical approach by concentrating on networks with regular topologies and (static and random) uniform all-to-all traffic. These assumptions are idealizations, nonetheless they keep the analysis tractable and provide us insights into more complex problems and they act as points of departures for the analysis of more realistic scenarios (such as irregular networks and non-uniform traffic) in the later part of this thesis.

The search for the scalable fiber connection architecture hinges on analyzing the tradeoffs among expensive network resources. In our parametric, first-order, and homogeneous cost model, the constituent parts, which are closely related to fiber topology, are fiber cost and switching cost. To build a network, one can support lightpaths by laying down direct fiber connections among all sourcedestination nodes. This design obviously requires minimal switching resources but maximal amount of fibers. Another way to establish lightpaths is by hopping through one or more nodes. Such a design requires less fiber connections but more switching resources. As such, the optimal connectivity of a fiber connection topology is determined by the fiber-to-switching cost ratio. Further, we show that the amount of switching resources used at nodes is proportional to the average minimum hop distance (for regular topologies and uniform traffic). To support the same set of (uniform) demands, we show that regular topologies with the smallest average minimum hop distances have lowest fraction of pass-through traffic and thus require less switching ports.

We also investigate designing networks that are robust to demand uncertainties, which are caused by diversification of services, changing of usage patterns, and data-dominated traffic in the metro environment, etc. We present a framework to assist network designers to dimension optical optical MAN,
incorporating uncertainties in demands. In this framework the interplay among topology design, resource provisioning, and routing are analyzed based on two stochastic optimization models that use probability distributions of demands as inputs. In one model, the weighted sum of network installation cost and expected penalty cost for unsatisfied traffic is minimized. In another model, the network installation cost is minimized subject to certain service level requirements. The optimization results enable us: (1) to identify the Generalized Moore Graphs as the physical architectures that are most robust (in cost) to demand uncertainties among rich classes of regular topologies, assuming the (random) uniform all-to-all traffic, and (2) to provide analytical references on how optimal dimensioning, network connectivity, and network costs change as functions of the designer's level of risk aversion, service level requirements, and probability distributions of the demand.

**Development of Two Network Topology Management Algorithms**

Network topology management via helper node trajectory control is a key aspect of the proactive mobile wireless network architecture. In general, there is a tradeoff between the number of helper nodes needed and algorithmic complexity and with the amount of network state information needed. For networks operating in a planar region, determining the minimum number of helper nodes needed and their locations at any instance in time is an NP-complete problem. We have developed two polynomial-time approximation algorithms based on minimum spanning trees with channel link states as weights on the edges of the trees. These algorithms range from centralized with full network state information to partially distributed with local link monitoring and performance within a small numerical multiplier of the optimum.

**Feasibility Study of the Proposed Network Architecture**

Since the proposed architecture spans several technology areas, we have examined all the building blocks to identify potential technology bottlenecks and enablers. It has been found that, in most cases, current technologies are sufficient for small network operations on the order of tens of nodes. As robots and small autonomous aerial vehicles become more practical, versatile, and robust, these devices can help to connect larger networks. We identify and propose technology enablers in two areas where existing technologies are deficient:

(a) Node localization in indoor environments -- Signal obscuration and multipath present significant challenges for indoor localization using narrow-band systems. Based on signal measurements from an ultrawide-band radio testbed in an indoor environment, we have compared location estimation error based on time-of-arrival (ToA) and received-signal-strength (RSS) for a variety of wireless beacon placement configurations. The results indicate that sub-meter location estimation accuracy is possible using wide-band ToA ranging. An important factor in this case is that the bandwidth is wide enough so that the multi-paths can be resolved.

(b) Channel prediction -- In the proposed architecture, it is necessary to estimate future link channel states even if nodes are mobile. Given node locations and predicted trajectories, future channel states may be estimated with the aid of physical and signal attenuation maps of the operating region. Physical maps of outdoor and indoor environments are typically available through overhead intelligence and floor plans. Using a neural network predictor, we have shown that signal attenuation maps can be constructed off-line using prior signal measurement data and quickly updated on-line when more channel state measurements are available.
**Future Optical Network Architectures**

Optical networking technology is poised to make significant contributions in next-generation data network architecture because of: (i) the enormous viable data bandwidth of optical fiber, and (ii) the ability to perform simple operations (e.g., switching) in the optical domain “in bulk”, leading to high-rate services which are independent of bit rate, format, and protocol. With the ubiquitous deployment of WDM technology in core networks in recent years – capitalizing on property (i) – long-haul transmission has become cheaper than routing and switching at core node routers. To continue reaping the economic benefits of optical networking technology, property (ii) of optical networking technology must be exploited via optical access and some form of optical switching and routing for large transactions. This would amount to a significant network architecture change – not mere substitution of optical components for electronic ones. The consequence of such a shift towards optical networking technology is that most architectural elements of networks – from the physical layer to higher layers, as well as network management and control (NMC) – must be rethought at the most fundamental level. Since NMC expenses can constitute a significant portion of the cost of a network, its cost-optimization is critical to ensure that it does not negate the other economic benefits of employing optical networking technology.

The research objective is the creation of an optimized, heterogeneous optical network architecture, comprising current and future technology building blocks, that realizes the full potential of optical technology and that will be able to support exponentially increasing future bandwidth demands.

The approach to developing an optimal optical network architecture will involve a restructuring and optimization of the existing network layer structure by: (i) treating architecture, protocols, and the physical layer as a single entity with strongly interacting, but distinct subsystems, and (ii) employing foreseeable technology as well as suggesting revolutionary hardware technology to exploit the benefits of optics wherever possible. The resulting intelligent optical network will be dynamically reconfigurable, and will enable various new applications by seamlessly optimizing network performance for all types of data traffic. Based on a system-wide optimization, the most efficient switching, routing and transport mechanisms will be developed, which we anticipate will include electronic packet switching as an important overlay atop a much higher-speed network.

The enabling architectural concepts in our research are: (i) optical flow switching (OFS) and its implications on physical and higher layer architectures, and (ii) impairment aware routing.

**Impact of Signal Processing Energy and Large Bandwidth on Infrastructureless Wireless Network Routing and Scalability**

Throughput scaling and optimal hop-distance of interference-limited wireless networks have been well characterized in literature. For some emerging wireless networks, throughput may be more limited by battery energy rather than by interference. In characterizing throughput scaling and optimal hop-distance of such power-limited networks, prior work have invoked a zero signal processing energy assumption, which led to the belief that “whispering to the nearest neighbor” (WtNN, with the average number of hops per source destination pair increasing with increasing node density) achieves the optimal throughput scaling, which increases with increasing node density. We show that this believe must be modified for power-limited networks when signal processing energy is not an insignificant factor. In fact, for a power-limited network with nodes uniformly randomly distributed in a bounded region, taking (i.e. does not increase or decrease with increasing node density) number of hops is throughput, energy, and delay optimal, achieving pairwise throughput, energy per bit, and packet delay under uniform traffic, whereas WtNN is strictly suboptimal, achieving a pairwise throughput, which decreases with increasing node density.
density. In addition, we show that a constant characteristic hop-distance of dchar simultaneously achieves the pairwise throughput scaling and minimum network energy consumption for random networks.

**Non-Adaptive Fault Diagnosis Schemes**

In non-adaptive fault diagnosis schemes, instead of sending optical probing signals sequentially, a pre-determined set of probing signals are sent in parallel to probe the network state of health. so that the number of probing steps is always one. In addition, compared to the probabilistic failure model (i.e., each link fails independently and no upper bound on the number of failures) used in our previous work, we also assume a worst-case failure model in that the number of simultaneous failures is upper bounded by a constant. Under such a framework, the design objective is to minimize the number of parallel probes for non-adaptive fault diagnosis schemes, so as to keep the fault diagnosis cost low.

The fault detection methods are based on techniques from the field of combinatorial group testing (CGT), where defected samples are identified through a set of parallel testing on different combinations of unknown samples. In our work, we propose a variant of classical CGT in which the valid tests are determined by the structure of a graph. In the all-optical network context, this graph corresponds to the network topology, and the constraint on valid tests is due to the fact that lightpaths can only traverse a set of interconnected edges. We formally analyze the number of tests needed for certain interesting classes of graphs (e.g., ring, bus, tree, 2-D grid, and complete graph), and even arbitrary graphs. We find out that the number of probes needed depends on the topology. In some cases, we can give matching upper- and lower-bounds on the number of tests needed. The fault diagnosis schemes have a common theme, which suggests a practical rule-of-thumb for efficient fault diagnosis schemes: a fault-free sub-graph in the network topology should be identified, and used as a “hub” to diagnose other failures in the network.

**Performance-Cost Tradeoffs of Optical Transport Architectures**

We have studied the optical flow switching (OFS) architecture in detail [3] and compared it to other optical transport network architectures – namely, electronic packet switching (EPS), optical burst switching (OBS) of which Tell-and-Go (TaG) is a special case, and GMPLS [1,2,4]. OFS provides dynamic and fast changing capacity to meet bursty high-volume user demands. With OFS, an (offband) signaling protocol will be employed by users to request lightpaths for their transaction durations, after which the network sets up an end-to-end lightpath for the duration of the transfer (>100 msec). When the transaction is over, the network resources are then relinquished for use by other users. Our study was motivated by our hypothesis – which was corroborated – that, for large transactions, optical flow switching is the right choice of architecture.

In the initial study of the different optical network architectures, we characterized their achievable throughput (i.e. capacity region) when used solely as a transport mechanism in the WAN. Results indicate that EPS maximizes capacity followed by OFS and GMPLS, followed finally by TaG and OBS.

These results, while telling, are limited in impact for several reasons, including (1) the absence of a concrete cost metric, and (2) that the local- and metro-area network were suppressed. Our next studies addressed these two shortcomings.
We conducted a throughput-cost comparison of a simple, yet scalable, multi-tiered optical network comprising two groups of users, each in a distinct metropolitan-area network (MAN), which wish to communicate over a wide-area network (WAN), as drawn below. The network cost model focused on initial capital expenditure: transceiver, switching, routing, and amplification costs. Our network model, though simple in that it only considers the communication of two sets of users across a WAN, is a building block for more complex network topologies, and, more importantly, captures the essence of the throughput-cost tradeoffs of these more complex networks.

The throughput-cost comparison of the four network architectures, using cost and architectural parameters which reflect the state of present-day networks, indicates that each architecture is optimum for a range of user rates. EPS and EPS/GMPLS dominate for lower rates because a small amount of electronic equipment is necessary to support the aggregate traffic; whereas, for OFS and TaG, expensive tunable, long-haul transceivers are always required at each end user. On the other hand, at high data rates, regardless of the number of users, OFS always dominates, implying that OFS is the most scalable architecture of all. In the high user data rate regime, aggregate traffic is always high, so requiring electronic equipment to support this traffic in the network -- even if only in the MAN -- is expensive. We note that there does not exist a regime of optimality for TaG since the low cost of scheduling in OFS yields great performance benefit relative to the otherwise identical TaG architecture.

**Proactive Wireless Networks**

The objective of this program is to develop a Proactive Mobile Wireless Network paradigm for next generation infrastructureless wireless networking to guarantee critical services to users with time deadline constraints. In contrast to existing mobile ad hoc wireless networks where frequent network disconnections and greatly degraded services may occur due to fluid changes in the location and composition of wireless devices in combat theatres, a proactive mobile wireless network actively maintains network connections to ensure continuous communication and timely delivery of mission-critical information. Such capabilities will be necessary and crucial for networks that operate under extreme operating scenarios, such as small unit operations, search and rescue, and urban warfare. In the initial phase of our study, we completed the following:

1. Feasibility study of the proposed network architecture.
2. Quantification of network gains.
4. Impact of signal processing energy and large bandwidth on infrastructureless wireless network routing and scalability.

The proposed Proactive Mobile Wireless Network architecture consists of the following primary components:

1. User location, movement trajectory, and communication channel state estimation for network disconnection prediction.
2. Adaptive deployment and movement command of helper nodes. These are additional wirelessly-enabled devices deployed with the single purpose of network connection maintenance. Examples of helper nodes include navigational robots or vehicles that plan their trajectories to connect user nodes where connections are most needed, or balloons and other aerial vehicles...
carrying communication relays that hover and drift above a region to provide wider communication coverage.

**Quantification of Network Gains**

The key architectural questions we want to address are: what helper node capabilities are needed in terms of mobility and communication and whether the increased complexity of the proposed architecture is justified. Using a simple random network model, we have quantified the probability of connection, and throughput, delay and energy gains for proactive mobile wireless networks under different helper node deployment schemes. It is found that for some network scenarios, even a few strategically placed mobile helper nodes with the same communication capabilities as user nodes can significantly improve network connectivity. For networks with sparsely distributed user nodes, aerial helper nodes are better than terrestrial ones and for networks with densely distributed user nodes, helper node mobility does not have significant gains over fixed helper nodes. For networks with moderately distributed user nodes, orders of magnitude savings in the number of helper nodes can be achieved by using mobile helper nodes compared to randomly deploying fixed helper nodes. In all cases, having more helper nodes will further improve throughput, delay, and energy with a more favorable throughput-delay tradeoff compared to networks with user nodes alone. In addition, strategically placing helper nodes can attain the minimum network energy consumption achievable for wireless networks.

**Claude E Shannon Communication and Network Group (CNG)**

The mission of the Claude E Shannon Communication and Network Group at the Research Lab of Electronics (RLE) is to be an international leader in research, education, and development in the communication and network fields.

The research mission is to address in a rigorous manner the fundamental problems affecting current communication and network systems and to influence the development of future systems. This research will be multi-disciplinary, applying the tools of mathematics, algorithms, system engineering, physics, device technology, and hardware system architectural constructs.

The education mission is to help create tomorrow’s academic and industrial leaders in the communication and network fields. The objective is to mentor students not only to help solve deep and fundamental problems from current and future technology, but also to learn the engineering art of identifying important problems and critically assess the main technological challenges.

The development mission is to interact with industry and government at many levels, to ensure the relevance of academic modeling, the professional development of students, the effective transfer of technology and to create an environment in which novel new systems can be created and evaluated.

Finally, the group aims to pursue its research, educational, and development missions in an open, supportive and inclusive research environment. The group will use Claude Shannon’s research career as its inspiration for far-reaching fundamental research to build a framework for the technical problems of tomorrow.

A major theme of the group is the pursuit of research that cuts across multiple disciplines. We believe the forefront of this area is at the interface of traditional quantitative communication and network research and adjacent areas such as computer science, physics, device, system design and
demonstration, operations research, economics and management. Examples are optical, wireless and satellite networks. Thematic research provides a venue to apply the fruits of basic research to real world problems, act as a reality check to abstractions and models made in fundamental theoretical research and as a source of new and interesting problems. A significant component of our research is the creation of new architectures guided by the understanding of technology and fundamental system limits and the realization and validation of these architectures with hardware and algorithms and system demonstrations. As such, we work closely with industry to extend our research reach and impact beyond the academic boundary.

**Satellite Networks and Architectures**

This research project will address the architecture designs for efficient data communications over (satellite systems) and especially when they are interconnected with terrestrial fiber and wireless systems to form a heterogeneous global Internet. There are three main components to this research:

1. Adaptive power and rate control techniques for the satellite systems over time-varying channels to achieve greatly improved data throughputs
2. Efficient routing algorithms over a time-varying integrated and heterogeneous global network for maximum resource utilization, especially the space segments.
3. Efficient congestion control algorithms at the transport and network layers for an integrated satellite/terrestrial network.

The satellite network of the future will have the following properties:

(a) Streams as well as bursty transactions.
(b) Predictable and unpredictable traffic changes with different quality of service requirements.
(c) Time varying channel capacities and qualities due to weather and dynamic power and beam allocations.
(d) Contending user applications that require dynamic resource allocation and reconfiguration with some rejection.
(e) Relatively cheaper space backbone Vs. up and down links.
(f) Possibility of shared processing in space, as well as high capacity memories.

In the light of these unusual properties, this research program studied the following network architecture design problems:

(a) Dynamic satellite connection topologies and node switching architecture, including reconfiguration of lasercom backbones connections subject to shifting traffic demands and up-and-down link adaptations; node switching architectures to deal with streams as well as bursty transactions.

(b) Routing, flow, and congestion control of stream and bursty traffic\Internetworking architecture with terrestrial networks and airborne platforms from Layer 1 to Layer 4 with the possibility of including the Application Layer, with particular attention given to the essential differences between space and other terrestrial and airborne networks, such as Doppler, propagation delays, and channel conditions.

(c) Network management and control as a distinct architectural focus that addresses the space environment and end-to-end networking across disparate subnets.
(d) Architectural constructs that lend themselves to evolution over time as technology and needs evolve. Especially notable is the revolution in relative capabilities for processing, storage and data transfer as they affect architectural considerations.

If the backbone transport has enough data rates or in the case of analog links enough fidelity in the transport of amplitude and phase, then there is the possibility of long baseline beam forming and interferometry.

Long base-line interferometry increases receiver dynamic range and sensitivity and in the case of space-borne applications, putting processing in space substantially reduces the downlink capacity requirement. This is a major benefit for space systems where down link resources are very expensive.

For terrestrial wireless applications, dynamic range extension is critical for the support of mobile users that pass through deep multi-path fades. The possibility of large scale frequency re-use is also a huge economic incentive to wireless operators.

This technique is not currently available because it needs either very high data rate digital or very high fidelity analog in the backbone. With fiber networks and the advent of optical cross-links in space, this will be possible in the future.

PROF. ANANTHA P. CHANDRAKASAN
Joseph F and Nancy P Keithley Professor of Electrical Engineering
Director, Microsystems Technology Laboratories (MTL)
http://www-mtl.mit.edu/~anantha/index.html
http://www.rle.mit.edu/rleonline/People/AnanthaChandrakasan.html
http://www.rle.mit.edu/rleonline/People/AnanthaChandrakasan_pubs.html


A High-Density 45-nm SRAM Using Small-Signal Non-Strobed Regenerative Sensing
High-density embedded SRAMs are critical enablers of the tremendous integration trends benefiting integrated circuits every technology node. Their wide use of aggressive minimum-sized features, however, severely aggravates variability, leading to numerous limitations across the entire array. Some of the most critical among these include highly degraded static-noise-margin (SNM) and cell read-current due to the use of small bit-cells; the need to increase sense-amplifier area in order to reduce its variation and input-offset to withstand the lower read-currents; and finally, excessive margining in the sense-amplifier strobe signal, which is required to overcome its severe tracking divergence across operating corners, with respect to the array read-path.
In order to simultaneously address all of these issues, we present the non-strobed regenerative sense-amplifier (NSR-SA). It performs very simple offset compensation to overcome the sense-amplifier offset-area trade-off without significantly loading the high-speed nodes. The resulting improvement in stability, even in the presence of extreme variation, implies that a small cell read-current can be accommodated for the same array performance, and, accordingly, the bit-cell can be optimized for other parameters, such as read SNM. Lastly, the presence of stable internal voltage references, generated thanks to the offset compensation, is exploited to trigger self-regeneration with respect to the input bit-line voltage itself, rather than to an explicit external control path. The test-chip, fabricated in 45-nm CMOS, employs high-density 0.25µm² bit-cells. Measurements from 53 die show an improvement in the sigma of the delay distribution by a factor of four compared to a conventional sense-amplifier, confirming the benefit of offset-compensation and self-regeneration.

**SRAM Design for Ultra-Low-Power Systems**

Low-power circuit design has been an important research area because of the ever-increasing need for longer battery life in energy-starved applications. Most digital systems require on-chip memory blocks that dominate not only area but also power consumption. Hence, lowering SRAM voltage is critical. First, this reduces the active energy, which is given by CVDD². The total energy makes a minimum around 400mV because of the opposing trends in the active energy and leakage energy components. Second, leakage-currents also decrease at lower supply voltages, resulting in reduced leakage-power. The leakage power decreases by ~50X over the range. This significant decrease is due not only to scaling in VDD but also to alleviation of drain-induced barrier lowering (DIBL).

Designing functional SRAMs at lower supply voltages is, however, extremely challenging due to the increasing effects of local variation with device scaling. To maximize density, the bit-cell is designed to be very small, aggravating its variability. Hence, as the supply voltage decreases, read and write failures begin to be highly prominent. Peripheral assists to address these and new bit-cell topologies have been proposed recently. However, architectural innovations are also required.

Operating voltage of an SRAM is often bounded by the performance requirement of the system. In such a scenario, the operating voltage can be brought down only if the performance of the SRAM is improved. Since the sense amplifier is in the critical path, its offset directly determines the discharge time, and hence a larger offset translates into a longer access period. In order to acquire the same performance at a lower VDD, sense-amplifier offset voltage should be analyzed. An offset compensation scheme that would trim the reference voltage value to minimize the offset can be implemented. This scheme should be implemented with a reasonable area overhead in order to be applicable to SRAMs.

**A Highly Digital, Resolution- and Voltage-Scalable SAR ADC**

In energy constrained systems such as wireless sensor nodes or mobile electronics, it is desirable to have analog-to-digital converters (ADC) that can operate in the sub-threshold regime to minimize energy during long standby periods but can also dynamically elevate their performance to meet system demands. In this work, a highly digital, energy-efficient successive approximation register (SAR) ADC with scalable resolution from 5 to 10-bits is being designed. Recent SAR ADCs have achieved energy efficiencies on the order of a few fJs per conversion step, but only at a fixed resolution. The main challenge in designing a scalable ADC is maintaining its energy-efficiency across all resolutions.
This SAR ADC consists of a comparator, a digital-to-analog converter (DAC) and digital control logic to implement a binary search algorithm. Clock gating is used to enable sample rate scaling from 1-MS/s down to 0. Special techniques are used to deactivate extraneous circuitry as resolution is reduced to maintain energy efficiency. Often, this scalability involves using analog switches at critical nodes and must therefore be carefully designed, especially at low supply voltages.

Lastly, voltage scaling is used to maintain a constant energy efficiency as the resolution is reduced. Recently, SAR ADCs operating on a 500-mV supply have been reported. This ADC will be designed to operate at 10-bits at 1-V, down to 5-bits at 400-mV.

**An AES-Based Energy-Efficient Encryption Processor with Resistance to Differential Power Analysis Attacks**

Security concerns for transmission or storage of data by battery-operated wireless systems require the development of an energy-efficient encryption processor. However, even with the security ICs, core information can be discovered by attackers since the ICs are vulnerable to side-channel attacks. Among all the side-channel attacks, differential power analysis (DPA) attack is effective in finding a secret key. Measuring the current from power supply and then performing statistical analysis of the measured power traces can lead to discovery of the secret key. Therefore, development of an energy-efficient encryption processor that is immune to differential power analysis attack is required for the secure transmission and storage of the data in battery-operated security ICs.

The Advanced Encryption Standard algorithm is a block cipher that converts 128-bit plaintext to ciphertext with selectable key lengths (128, 192, or 256 bits). The algorithm is organized as a repeated “round transformation” that includes four types of sub-operations, i.e., “SubBytes,” “ShiftRows,” “MixColumns,” and “AddRoundKey.” For the design of an energy-efficient processor with performance requirement, two architectural approaches can be used with voltage scaling. Since a total of 32 bytes is manipulated in one round of transformation, parallel operation of each byte can compensate for the reduced speed that results from the supply voltage scaling. Pipelining also helps maintain the throughput even with the reduced supply voltage.

The DPA attack is based on the asymmetry in power dissipation, depending on the input data. Dynamic differential logic consumes the same dynamic power regardless of any input data, since during the precharge phase, one node is always precharged to VDD, and during the evaluation phase, one node is always discharged to ground. Resistance to DPA attack with dynamic differential logic, however, comes at the expense of increased power dissipation. Therefore, the trade-off between security and power dissipation should be examined carefully and optimized for the specified design purposes.

**On-Chip Voltage-Scalable Switched-capacitor DC-DC Converter**

Minimizing the energy consumption of battery-powered systems is a key focus in integrated circuit design. Dynamic voltage scaling (DVS) and sub-threshold operation are popular methods to achieve energy efficiency in systems that have widely variant performance demands. However, to realize the full energy benefits of voltage scaling, an efficient voltage-scalable DC-DC converter is of great importance. DVS systems also often require multiple on-chip voltage domains with each domain having specific power requirements. A switched-capacitor (SC) DC-DC converter is a good choice for such battery operated systems because it can minimize the number of off-chip
components and does not require any inductors, thereby reducing the overall DC-DC converter volume and cost.

A switched-capacitor DC-DC converter implemented in 0.18µm CMOS employs Pulse Frequency Modulation (PFM) to achieve a voltage regulation. In this mode of control, the converter stays idle till the load voltage (VL) falls below a user-defined reference voltage (VREF), at which point the comparator enables the switch matrix to transfer one charge packet to the load. The switched capacitor DC-DC converter employs on-chip charge-transfer capacitors and can provide scalable load voltages from 0.3V to 1.1V. In order to maintain efficiency over this voltage range, the converter employs 5 different gain settings (G<0:4>) which help in minimizing conduction loss. The automatic frequency-scaler block helps to adjust the frequency of operation and the size of the switches (enW<0:1>) within the switch matrix, with changes in load power. This helps in scaling the switching losses as the load power varies. A divide-by-3 switching scheme was employed in the converter to reduce the parasitic bottom-plate losses and improve efficiency. Also, the all-digital control circuitry used in the converter consumes no static power. The voltage-scalable SC DC-DC converter with integrated on-chip charge transfer capacitors was implemented in National Semiconductor’s 0.18µm CMOS process and consumed an active area of 0.57mm(2). The converter achieved above 70% efficiency over a wide range of load powers from 5µW and 1mW, while delivering load voltages from 300mV to 1.1V.

A modified version of this design was implemented as part of a 65 nm sub-threshold microcontroller system. The DC-DC converter in the microcontroller occupied just 0.12mm(2) in area and was able to achieve 75% efficiency at a load voltage of 500mV with the microcontroller as the load.

Self-Powered Electronic Systems

A micro energy processor that could harvest energy from vibrations, temperature differences, solar panels, and radio waves could wirelessly provide the power to run Bluetooth headsets or implanted medical devices.

This project will try to develop control systems for "self-powered" devices, such as biomedical sensors or therapeutic devices that generate their own electricity from the user's movements or body heat so that they never require battery replacement.

A 65-nm, Sub-V(t) Microcontroller with Integrated SRAM and DC-DC Converter

Aggressive scaling of the power supply to below the device threshold voltage (Vt) is a compelling approach for energy minimization in digital circuits. Although circuits exhibit slower speeds at low supply voltages, the trade-off remains attractive for energy-constrained systems with relaxed throughput constraints. However, effects of process variation become more prominent at low supply voltages, impacting functionality. A 65-nm sub-Vt microcontroller demonstrates several approaches to enable operation down to 300mV. In sub-Vt, logic gates no longer exhibit rail-to-rail voltage swings due to variation and reduced ratio of on-to-off currents. A standard cell library design methodology increases device sizes appropriately to mitigate these effects. Moreover, circuit delays exhibit order-of-magnitude higher variability at low voltages. Conventional timing analysis approaches that treat delays as deterministic are insufficient. Instead, a variation-aware methodology combining simulation and analysis was developed to verify hold-time constraints.

The SRAM represents a dominant portion of power and area in this system. Therefore, energy and leakage reduction through voltage scaling is highly desirable. In conventional 6-T SRAMs, Vt
variation causes severely degraded read-current and increased cell instability, limiting the minimum functional voltage. The SRAM in this chip employs an 8-T bit-cell to address these limitations. Further, peripheral circuit assists enforce the relative device strengths needed for read and write functionality, even in the presence of significant variation. A fully integrated, switched-capacitor DC-DC converter provides highly efficient power delivery at the low voltage and power levels required by energy-constrained systems. Featuring multiple gain settings and efficient control circuitry, the DC-DC converter can deliver variable load voltages and achieves above 75% efficiency while supplying 500mV in the range of 10µW to 250µW. The microcontroller chip was fabricated by Texas Instruments.

Algorithms and Architectures for Ultra-low-power Video Compression

Multimedia applications, such as video playback, are becoming increasingly pervasive. Since the platforms are often energy-constrained devices (cell phones, IPODs), the user experience is enhanced by extending the battery life during video decoding. The latest video coding standard is H.264, and it is used in DVB-H and HDTV. While it provides a 50% improvement in compression efficiency over previous standards, this coding efficiency comes at the cost of increased decoder complexity of 4X over MPEG-2 and 2X over MPEG-4 Visual Simple Profile. This increased complexity translates to increased energy consumption, which is a critical concern for mobile and handheld devices.

This project aims to build an ASIC decoder that exploits techniques such as pipelining, parallelism, ultra-low voltage operation, and ultra-dynamic voltage scaling. For instance, the IDCT computation can be parallelized. In video decoders, memory consumes a large portion of overall system power. As a result, the number of redundant memory transfers must be minimized and caching data in on-chip SRAMs/registers should be explored. Using these techniques, the goal is to minimize system power, as compared to previously published decoders. In addition to optimizing the hardware architecture of the H.264 decoder, we will also focus on the design of future video coding standards, e.g., “H.265”. We envision that future algorithms will account for the energy and complexity costs of their hardware implementations. By incorporating the energy-awareness into the algorithm, future video coders can provide an explicit energy/PSNR trade-off, along with the existing bitrate/PSNR trade-off curves.

An Ultra-Low Power CMOS RF Transceiver for Medical Implants

Until recently, few medical implantable devices existed and fewer still provided the capability for wireless transmission of information. Most devices capable of data transmission did so through inductive coupling, which requires physical contact with the base-station and allows for only low data rates. In 1999, the FCC created the Medical Implant Communications Service (MICS) band in the range of 402-405 MHz specifically for medical telemetry. The MICS band plan allows for RF communication between a medical implant and a base-station that is up to two meters away. This research seeks to design a transceiver specifically optimized for low-power, short-distance data transmission in a temperature-regulated environment, i.e., the human body. We do this by pushing as much complexity as possible out of the implant and into the base-station, taking advantage of the attributes of the environment, such as temperature control and slow transients, and incorporating the antenna into the oscillator for reduced power and improved performance. By optimizing the transceiver for reduced volume and power, we hope to extend the battery lifetime and functionality of medical implants for greater comfort and benefits to patients.

We propose a simple, almost all-digital transceiver comprising a direct modulation frequency-shift keying transmitter and a super-regenerative receiver. The transmitter is composed of a
digitally-controlled oscillator (DCO) and simple digital logic; the receiver uses the same DCO, a quench oscillator, an envelope detector, a comparator and simple digital blocks. Data is transmitted by directly modulating the frequency of the DCO through a capacitor bank. The frequency deviation constant is digitally set through a serial-to-parallel interface such that digital data composed of ones and zeros shift the DCO frequency by a desired amount. We linearize the digital-to-frequency relationship of the DCO by pre-distorting the capacitor banks used to tune the frequency and the frequency deviation constant of the transmitter. Instead of driving the antenna with a matched power amplifier, we exploit the low radiation power requirement of MICS to incorporate a loop antenna into the DCO. The inherently high Q of the antenna leads to improved noise performance for a given amount of power.

The SRR receives on-off keying (OOK) data and determines whether a one or a zero was sent by measuring the amount of time required for the envelope of the DCO output to reach a threshold. Input signals with large amplitudes and strong frequency content near the DCO’s resonant frequency result in faster startup times. A digital counter determines the startup time and compares it to a threshold.

The design was implemented in IBM 90-nm CMOS. The transmitter consumes under 350µW and meets MICS mask specifications with data rates up to 120kbps. The receiver consumes under 400µW and achieves a sensitivity of -99dBm or better at data rates of 40kbps, or -93dBm at data rates of 120kbps. The DCO tunes 24MHz in frequency steps smaller than 2kHz.

**Design and Characterization of CNT-CMOS Hybrid Systems**

Carbon nanotubes (CNTs) are nanometer-diameter cylinders formed from rolled-up graphene sheets. CNTs have found widespread interest due to many of its excellent electrical properties. In particular, the low density and high electron mobility of CNTs make them attractive for electronic applications. Our investigation of hybrid CMOS-CNT systems attempts to take advantage of the superior properties of CNTs while building on top of existing CMOS technology.

We propose an integrated chemical sensor system to verify the concept of a CNT-CMOS hybrid system design. The CNT changes its conductance when exposed to certain chemicals, and thus we can effectively use CNTs as resistive chemical sensors. Room-temperature operation of the CNT sensors makes them an appealing candidate for low-power chemical sensor application. However, poor control over the local and global variation of CNT devices, the resolution requirements in resistance measurements, and the changes in resistance due to specific chemicals implies a large dynamic range in the front-end circuitry. We investigate energy efficient architectures to accommodate the specification. Chip fabrication is done by National Semiconductor.

Another system of interest is a DC-DC power converter circuit. Near ballistic transport behavior of CNTFET makes it a potential energy-efficient candidate in power applications. In addition, the power transistor size could be greatly reduced if CNTFETs can replace the CMOS power transistors and the CNTs are aligned. Currently, we are looking into ways to model CNTFET behavior and fabricating CNT devices that can support large currents.

**Minimum Energy Tracking Loop with Embedded DC-DC Converter in 65-nm CMOS**

Minimizing the energy consumption of battery-powered systems is a key focus in integrated circuit design. Switching energy of digital circuits reduces quadratically as VDD is decreased below VT, i.e., sub-threshold operation, while the leakage energy increases exponentially. These opposing trends result in a minimum energy point (MEP), defined as the operating voltage at
which the total energy consumed per operation (Eop) is minimized. The MEP can vary widely for a given circuit depending on its workload and environmental conditions, e.g., temperature. Energy savings of 50 - 100% are demonstrated by tracking the MEP as it varies, and even greater savings can be achieved in circuits dominated by leakage.

The energy-minimization circuitry consists of a buck converter that operates in the Pulse Frequency Modulation (PFM) mode. The digital circuit (FIR filter), which operates at the VDD set by the converter, is clocked by a critical path replica ring oscillator. The energy-sensor circuitry determines the energy consumed per operation at different operating voltages. Based on the energy per operation at a given operating voltage obtained from the energy-sensing circuit, an energy minimization algorithm changes the reference voltage to the buck converter suitably and the system approaches the minimum-energy operating voltage of the digital circuit using a slope-detection strategy. A test chip containing the minimum-energy tracking loop and the embedded DC-DC converter was fabricated in Texas Instruments' 65nm CMOS process. The area overhead of the minimum energy tracking loop which comprises the energy-minimizing block and the energy sense capacitors C1 and C2 is just 0.05mm2. The digital test circuitry operates at voltages as low as 0.25V. Energy savings of the order of 50 – 100% were measured while tracking the MEP as it varies with workload and temperature. The DC-DC converter was able to deliver load voltages between 0.25V and 0.7V with an efficiency > 80% at load power levels of the order of 1µW and above.

**Reaching the Optimal Mixed-Signal Energy Point**

Ultra-wideband radio can be used for very high data rate (>480 Mb/s) communication over short distances. For proper reception, the receiver requires a 500 MS/s analog-to-digital converter (ADC) with 4 bits of resolution. While flash is the typical architecture chosen, successive approximation register (SAR) ADCs feature superior complexity characteristics with similar amenability to deep submicron CMOS. Time-interleaving multiple SAR ADCs allows this long latency architecture to equal the throughputs necessary for UWB reception. A comparative energy model concludes that SAR should outperform flash above 5 bits of resolution in 0.18_m CMOS, with its energy advantage improving in more advanced technologies. The SAR architecture is particularly well suited to meet the challenges of design in deep submicron CMOS, including reduced voltage supplies, increased variability, and lower transistor output impedances. It uses only open loop amplification in a comparator, as opposed to the operational amplifier for the pipelined architecture. There is significant digital complexity on the critical path in a SAR converter, but digital power and speed directly benefit from the reduced feature sizes.

A prototype 500-MS/s, 5-b, 6-way time-interleaved SAR ADC has been designed and fabricated in Texas Instruments' 65-nm CMOS process. The prototype includes the split capacitor array that conserves charge between bit-cycles to lower the overall switching energy, and it settles faster because fewer capacitors switch during each period. The array also exhibits improved differential nonlinearity, with the same integral nonlinearity, which decreases the capacitor matching required to avoid missing codes. The ADC achieves Nyquist performance and consumes 6 mW from a 1.2 V supply.

An understated trend in ADC design is the significant impact of digital circuitry on performance and power, particularly at medium to low resolutions. Even in this advanced technology, half of the total ADC power is consumed by the digital circuitry. A genuine mixed-signal energy optimization that explicitly includes all of the analog and digital blocks, and their interactions, is...
being developed to minimize the power consumption of this ADC. The optimization uses coupled energy and behavioral models to explicitly define the analog/digital interactions and tradeoffs.

Reconfigurable Zero-Crossing-Based Analog Circuits

Switched-capacitor circuits can be used to implement many analog systems such as ADCs, DACs, filters, amplifiers, and integrators. In this research, a reconfigurable switched-capacitor system is proposed to implement different analog systems. Each switched-capacitor block can implement an integrator or a multiplier with a reconfigurable coefficient. Such a system will be useful for software defined radios and fast prototyping of analog circuits.

The design of such systems has not been practical since switched-capacitor circuits are op-amp-based. The design of reconfigurable switched-capacitor blocks with op-amp is very challenging if widely ranging speed, accuracy, signal-to-noise ratio (SNR), and power consumption space are to be covered. Many different op-amp topologies may be required to cover a large performance and configuration space. While new technology nodes provide transistors with higher ft, the design of op-amp is becoming more challenging as the supply voltage and intrinsic gain of transistors are decreasing. Recently, zero-crossing circuits to design ADCs were proposed. Zero-crossing circuits can replace the op-amp in traditional switched-capacitor design with a combination of a current source and a zero-crossing detector. The power consumption of zero-crossing-based analog circuits scales according to the operating frequency and required SNR. Zero-crossing circuits are used to implement the reconfigurable analog blocks needed for this research. The system can operate at different speeds and SNR requirements while the power consumption is kept at the optimum level.

PROF. HAE-SEUNG LEE
Professor of Electrical Engineering
Director, Center for Integrated Circuits and Systems (CICS)
http://www-mtl.mit.edu/researchgroups/cics/
http://www-mtl.mit.edu/researchgroups/hslee/
http://www-mtl.mit.edu/researchgroups/hslee/pubs.html

Hae-Seung (Harry) Lee’s research interests are in the area of analog integrated circuits, early vision circuits, fabrication technologies, and solid-state sensors. Professor Lee is a recipient of the 1988 Presidential Young Investigators' Award. He has served on a number of technical program committees for various IEEE conferences, including the International Electron Devices Meeting, the International Solid-State Circuits Conference, the Custom Integrated Circuits Conference, and the IEEE Symposium on VLSI Circuits. From 1992 to 1994 he was an associate editor for the IEEE Journal of Solid-State Circuits. Prof. Lee is a Fellow in IEEE and has been a member since 1988. Prof. Lee has been on the ISSCC Program Committee in 1998, 1999, 2000. He is the Director for MIT's Center for Integrated Circuits and Systems. Prof. Lee is also the Area III Chair.

Comparator-Based Circuits for HBTs

Recently, comparator-based switched-capacitor (CBSC) circuits and zero-crossing-based circuits (ZCBC) were introduced as a viable alternative to op-amp-based circuits. The use of op-amps in analog signal processing circuits is becoming more difficult due to the decreased intrinsic device gains and reduced signal swings obtained in scaled CMOS technologies. Op-amps rely upon high gain in the negative feedback mode in sampled data systems because the gain determines the accuracy of the output value. CBSC and ZCBC-based circuits replace the op-amp using a
comparator and a current source, and therefore do not require high gain and stability simultaneously as in op-amp-based circuits. Since comparators can be designed without the use of complementary devices, these techniques can be applied to a variety of transistor technologies. In this work, we explore the use of heterojunction bipolar transistors (HBTs) in comparator-based circuits for sampled data systems.

HBTs offer much higher device speeds than CMOS devices and have demonstrated the fastest transistor speeds to date with cutoff frequencies as high as $f_T=710$ GHz using a pseudomorphic InGaAs/InP HBT. Commercially, silicon germanium (SiGe) based HBTs have been developed with a cutoff frequency of $f_T=200$ GHz. The faster device speeds that HBTs offer can help meet the demand for very high speed, high-resolution analog-to-digital converters (ADC) for various applications including wireless and wireline communications and radar systems. HBTs also have a more constant $g_m/I$ ratio over the normal operating range, lower 1/f noise, and better device-matching of differential pairs than CMOS devices.

This project focuses on the development of innovative circuits and architectures to design a 12-bit pipelined ADC operating at 2 GHz using either an HBT-only or SiGe BiCMOS process. The first goal of the project is focused on adapting switched emitter-follower sample-and-hold circuits for switched-capacitor applications. Ultimately, the project will culminate in the design of a prototype ADC chip.

**A Zero-Crossing Based, 8b, 200MS/s Pipelined ADC**

Technology scaling is creating significant issues for switched capacitor circuit design. Decreasing device gain and voltage supplies make traditional implementations of high-gain, high-speed operational amplifiers (op-amps) increasingly difficult and less power-efficient. A comparator-based switched capacitor (CBSC) circuit technique was introduced in that replaces the functionality of an op-amp with a comparator and current source to help with these issues. The current source sweeps the output node with a voltage ramp until the comparator detects that the virtual ground condition has been realized. Whereas an op-amp-based implementation forces the virtual ground condition, CBSC circuits detect the virtual ground condition to realize the same precision charge transfer.

The comparator input in a CBSC implementation is a constant slope voltage ramp, and so the comparator performs a zero-crossing detection. This work generalizes CBSC by replacing the general-purpose comparator of CBSC circuits with a zero-crossing detector to realize new architecture called zero-crossing based circuits (ZCBC). Devices M1 and M2 make a dynamic zero-crossing detector that is fast, simple, and amenable to scaling. It draws no static current and thus realizes a power-efficient threshold detector. To improve linearity and output swing, the single current source of the previous design was split to create current sources I1, I2, I3, and I4. In this topology the capacitors are no longer charged through a series switch, so the associated non-linear voltage drop is eliminated. Furthermore, the traditional bit decision comparators in a pipelined ADC have been replaced with bit decision flip-flops for improved speed.

To demonstrate these techniques, an 8b, 200MS/s ZCBC pipelined ADC was implemented in a 0.18-um CMOS technology in an active die area of 0.05mm2. The differential non-linearity (DNL) and integral non-linearity (INL) are 0.75LSB8 and 1.0LSB8. The measured effective number of bits (ENOB) is 6.4b. It consumes 8.5mW (2.9/5.6mW analog/digital) from a 1.8V power supply. It draws only dynamic CV2f power as there are no statically biased circuits in the complete ADC. The corresponding figure of merit (FOM=$P/2fin/2ENOB$) is 510 fJ/step at 200MS/s. This
demonstrates best-in-class performance in terms of power-efficiency among other published ADCs in its class.

**High-Accuracy Pipelined A/D Converter Based on Zero-Crossing Switched Capacitor Circuits**

Technology scaling poses challenges in designing analog circuits because of the decrease in intrinsic gain and reduced swing. An alternative to using high-gain amplifiers in the implementation of switched-capacitor circuits has been proposed that replaces the amplifier with a current source and a comparator. The new comparator-based switched-capacitor (CBSC) technique has been implemented in two pipelined ADC architectures at 10MHz and 200MHz and 10bit and 8bit accuracy, respectively.

The purpose of this project is to explore the use of the CBSC technique for very high-precision AD converters. The goal of the project is a 100MHz 16 bit pipelined ADC. First, we are investigating multiphase CBSC operation to improve the power-linearity trade off of the A/D conversion. We are also developing linearization techniques for the ramp waveforms. Linear ramp waveforms require fewer phases, thus allowing faster operation. Techniques for improving linearity beyond using a cascaded current source are explored. A linear ramp generator, which decouples the current source from the output ramp through a Miller capacitor is proposed to improve the linearity of the ramp waveform in all phases. This ramp generator improves the range by improving linearity through compensation of the gate-to-source voltage of the current source without the use of a cascode. In addition it lends itself to a symmetric differential implementation for the final phase to ensure adequate noise rejection. At the target resolution of 16 bits, power supply and substrate noise coupling can limit the performance. We are studying their effects in CBSC circuits. For reduced sensitivity to power supply and substrate noise, we are developing a differential CBSC architecture. Other techniques that we are presently developing include power-efficient offset cancellation in comparators and exploiting a priori information from previous stages in the pipeline structure to increase linearity and speed.

**Ultra-High Speed A/D Converters Using Zero-Crossing-Based Circuits**

With an increasing need for higher data rates, both wireless applications and data links are demanding higher speed analog-to-digital converters (ADC) with medium resolution. In particular, this work will investigate ADC's with sampling rate up to 10 Gs/s with 6-8 bits of resolution. Time-interleaved converters achieve their high sampling rate by placing several converters in parallel. Each individual converter, or channel, has a delayed sampling clock and operates at a reduced sampling rate. Therefore each channel is responsible for digitizing a different time slice. This method requires that the individual converters, which make up the parallel combination, be matched. Mismatches and non-idealities, such as gain error, timing error, and voltage offset, degrade the performance. Therefore channel matching is an important design consideration for time-interleaved ADCs.

Although digital calibration can mitigate many of these non-idealities, timing mismatches are non-linear errors, which are more difficult to remove. At sampling rates up to 10Gs/s, digital calibration would consume a large amount of power. An alternative solution uses a global switch running at the full speed of the converter. This technique works well for medium-high speed ADC's. At higher speeds the ability to turn the switch on and off at the full sampling rate becomes a major challenge. We will investigate the applicability of the global switch technique in 90- or 65-nm CMOS technologies for 10Gs/s operation.
Power optimization is a major design consideration when implementing a time-interleaved ADC. We will lower total power consumption by exploring innovative technologies for implementing the individual ADCs in the channel, such as the zero-crossing based circuits (ZCBCs). The ADC topology was previously presented. In particular, this work investigates a fast, single-slope architecture. The faster each channel operates, the fewer channels are needed, hence lowering power in clock and buffer circuits. The primary emphasis falls on the development of highly power-efficient single-slope ZCBC architecture. Since the single slope architecture is more sensitive to non-idealities such as ramp nonlinearity, we are carefully studying the sources of non-idealities and develop clever techniques to address the accuracy issues.

PROF. JAE S. LIM
Professor of Electrical Engineering
http://www.rle.mit.edu/rleonline/People/JaeS.Lim.html
http://www.rle.mit.edu/rleonline/research/AdvancedTelecommunicationsandSignalPro

Profssor Jae S. Lim is a principal investigator in the Research Laboratory of Electronics (RLE) at the Massachusetts Institute of Technology (MIT). His research interests include digital signal processing and its applications to image, video and speech processing. He has contributed more than one hundred articles to journals and conference proceedings. He is the holder of more than 30 patents in the areas of Advanced Television Systems and Signal Compression. He is the editor of a reprint book, Speech Enhancement, and a co-editor of a reference book Advanced Topics in Signal Processing, published by Prentice-Hall in 1983 and 1987 respectively. He is also the author of a textbook Two-Dimensional Signal and Image Processing published by Prentice-Hall in 1990.

Advanced Telecommunications and Signal Processing (ATS) Group

The present television system was designed nearly 60 years ago. Since then, there have been significant developments in technology, which are highly relevant to the television industries. For example, advances in the very large scale integration (VLSI) technology and signal processing theories make it feasible to incorporate frame-store memory and sophisticated signal processing capabilities in a television receiver at a reasonable cost. To exploit this new technology in developing future television systems, the research areas of the program focused on a number of issues related to digital television design. As a result of this effort, significant advances have already been made and these advances have been included in the U.S. digital television standard. Specifically, the ATSP group represented MIT in MIT’s participation in the Grand Alliance, which consisted of MIT, AT&T, Zenith Electronics Corporation, General Instrument Corporation, David Sarnoff Research Center, Philips Laboratories, and Thomson Consumer Electronics. The Grand Alliance digital television system served as the basis for the U.S. Digital Television (DTV) standard, which was formally adopted by the U.S. Federal Communications Commission in December 1996.

The digital TV system based on this standard has been deployed successfully. In 2006, digital television receiver sales exceeded analog television receivers in both number and dollar volume in the U.S. The analog terrestrial TV service was discontinued in the U.S. in June 2009.

The standard imposes substantial constraints on the way the digital television signal is transmitted and received. The standard also leaves considerable room for future improvements through technological advances. Future research will focus on making these improvements. The digital television system is a major improvement over the analog television system. The next
major improvement over the digital television system is likely to be in the introduction of 3-D television. We are currently planning future research in this area.

**Transforms for Prediction Residuals in Video Coding**

To store or transmit a large amount of data involved in visual media, digital image and video compression technologies are utilized. For example, to transmit the HDTV signal in a bandwidth originally designed for analog television broadcast, compression by a factor of 70 is performed. Compression is achieved in part by exploiting temporal and spatial redundancies present in visual media. Temporal redundancy refers to the fact that there are often very small changes from frame to frame within a video sequence. Spatial redundancy, present in a single frame or an image, refers to the similarity or slow variations of picture elements in a small neighborhood.

Spatial redundancy in images is reduced by applying transforms on a small neighborhood of pixels. These transforms have the energy-compaction property, which means that a small number of transform coefficients are sufficient to capture the signal in that small neighborhood with adequate fidelity. Temporal redundancy is reduced by using motion-compensated prediction techniques. Typically, a frame is divided into small blocks, and each block is predicted from previously transmitted frames by searching them for a good match for that block. The difference between the prediction and the frame to be coded is often called the motion-compensation residual (MC-residual). In standard video encoders, the MC-residual is compressed in the same way as an image is compressed with the widely used JPEG image compression. Specifically, the same transform, the Discrete Cosine Transforms (DCT), is used. The MC-residual is intimately connected to images it has been obtained from. However, its spatial characteristics differ considerably from that of an image. This research focuses on developing transforms for the MC-residual, as well as other residuals encountered in video coding, such as the upsampling residual in scalable video coding and the disparity-compensation residual in multiview video coding.

The properties of the MC-residual have been studied by various researchers. The autocovariance of the MC-residual is modeled as a sum of a first-order Markov-process and independent white noise. This model reflects the relatively weaker correlation of the MC-residual compared to images in a simple and tractable way. The authors propose another compound model which fits the tails of the auto-covariance of MC-residuals better than the model A more complicated analysis resulting in a more complicated model. All these studies indicate that the statistical characteristics of the MC-residual have differences from the statistical characteristics of images. However, transforms accounting for these differences can often not be derived directly from such characterizations because most of these characterizations are rather complicated.

Recently, there has been a great deal of research on transforms that can take advantage of locally anisotropic features in images. Conventionally, the 2-D DCT or the 2-D Discrete Wavelet Transform (DWT) is carried out as a separable transform by cascading two 1-D transforms in the vertical and horizontal directions. This scheme does not take advantage of the locally anisotropic features present in images because it favors horizontal or vertical features over others. For example, the 2-D DWT has vanishing moments only in the horizontal and vertical directions. In these more recent approaches, transforms adapt to local anisotropic features by performing the filtering along the direction where the image intensity variations are smaller. This is achieved by resampling the image intensities along such directions, by performing filtering and subsampling on oriented sublattices of the sampling grid, by directional lifting implementations of the wavelet transform, or by various other means. Even though most of the work is based on the wavelet transform, applications of similar ideas to DCT-based image compression have also been made.
[8]. However these ideas have not yet been applied to modeling and compressing the MC-residual.

In this research, our goal is to develop transforms for the MC-residual as well as other residuals encountered in video coding, such as the upsampling residual in scalable video coding or the disparitycompensation residual in multiview video coding. Using insights obtained from the research on directionadaptive image transforms, we investigate how locally anisotropic features of images affect the MC-residual. We obtain an adaptive auto-covariance characterization of the MC-residual, which reveals some statistical differences between the MC-residual and the image. Based on this characterization, we have developed a set of block transforms that can be used to compress the MC-residual. Future research will focus on obtaining similar characterizations and transforms for the upsampling and disparity estimation residuals.

Transforms for Prediction Residuals in Multiview Video Coding

Multi-view coding algorithms exploit the redundancy of information between subsequent image frames and also between the different views of the scene. The subjective quality of the reconstructed video sequences produced by such algorithms should be sufficiently high. The major compression techniques currently used for stereoscopic and multiview video coding include disparity compensation, 4-D sub-band coding [3], global geometric warping and object-based schemes, which are for such specific applications as 3-D teleconferencing.

A major objective of multiview video compression/light field compression is to fully exploit the intra-view and inter-view coherence in the data set. The intra-view refers to the relationship among pixels within the same view, and inter-view refers to the relationship between pixels in views captured from different viewpoints. In addition, it is desirable to have a scalable representation of the video, which allows the system to efficiently adapt to varying storage capacities, transmission bandwidths, display devices, and computational resources by decompressing and rendering the video only up to a certain resolution, quality, or bit-rate requirement.

For two-view stereoscopic compression, the first left eye frame is often coded as an I-frame. Subsequent frames of the left-eye stream are predicted from the first frame using motion compensation and the right-eye frames are predicted from their corresponding left-eye frames using disparity compensation. Hence, the first frame of the left-eye stream is an I-frame and some additional frames are P-frames. In more sophisticated schemes, bi-direction predictions [1], similar to that in monocular streams, are often used. In light field compression, more complicated prediction schemes are exploited.

The global disparity is one of the major properties of the multiview video. The view disparity is similar to the temporal motion in the sense that they both represent the displacements between adjacent frames, whereas the properties and the inherent motion model are different. For example, it is well known that the disparity that represents the difference between two adjacent views is usually very compact. Therefore, a warping-based lifting transform can be used based on the assumption that the disparity between views can be well represented by a global disparity model. Since this assumption is not always true for the natural video due to the distortion of cameras and the scene depth, the practical solution should also consider the local disparity model.

Object-based coding of stereo sequences is an alternative to block-based schemes, since it can potentially produce fewer coding artifacts and provides a structural description of the scene useful
in many applications. The block-based approach has the advantage of simplicity and robustness, allowing more straightforward hardware implementations, but the subjective quality of reconstructed images may not be good in low bit rates. Comparing to the block-based approach, object-based schemes can alleviate the problem of annoying coding errors, providing a more natural representation of the scene, but require a complex analysis phase to segment the scene into objects and estimate their motion and structure.

Furthermore, important image areas such as facial details in face-to-face communications can be reconstructed with a higher image quality than with block-oriented hybrid coding. In addition, the ability of object-based coding techniques can describe a scene in a structural way, in contrast to traditional waveform-based coding techniques. Object-based approaches applied in coding of stereo image sequences have the additional benefit of conveying depth information, which may be computed directly from the images. Using the depth information the scene may be separated in layers and depth keying is possible. Also accurate 3D modeling of the scene structure may be achieved. However, modeling techniques proposed in the literature are often restricted to video-phone sequences where the scene structure is known a priori and knowledge-based parameterized models of face, arms, and body may be exploited. A more general approach exploits depth information.

In general, it is easy to see that each type of compression algorithm works well with classes of video frames with specific properties. In our research, we have developed an approach to combine various existing compression algorithms. Each algorithm works well with a relatively small class of images but with very good performance. The different algorithms are applied to each image and the algorithm that works best is selected for that image. This approach has a number of potential advantages over conventional methods where the same compensation and compression algorithm is used for all the frames in the video.

**Improvement of H.264 Using JPEG 2000 Technology**

JPEG is a commonly used still image compression standard developed in the late 1980s. It is widely used today for storing and transmitting digital images via the web. In the frequency domain, the image coefficients can be more efficiently compressed than in the spatial domain. JPEG uses a Fourier-related transform called the Discrete Cosine Transform (DCT) to convert images from the spatial to the frequency domain. Most of the loss in JPEG compression occurs during the quantization of the DCT coefficients. The coefficients are then entropy encoded for better compression.

A recent improvement on the JPEG standard is JPEG 2000. This new standard implements several new techniques to improve compression and image quality. One change is in the Fourier-related transform. JPEG 2000 uses the Discrete Wavelet Transform (DWT) instead of the DCT. The DWT reduces blocking artifacts at low bitrates. However, the DWT has more blurring artifacts. JPEG 2000 also uses a binary arithmetic encoding for entropy encoding. This allows a noninteger number of bits for encoding each coefficient, as opposed to Huffman encoding, used by JPEG, which requires an integer number of bits for each coefficient.

In our research, we are studying how to apply the techniques of JPEG 2000 to H.264/MPEG-4, a video encoding standard. In video compression, there are three types of frames: I, P, and B frames. P and B frames are encoded using motion compensation, a technique in which previously encoded frames are used to predict the current frame. The error between the actual and predicted
frame is encoded, not the frame itself. The I frames are coded independent of other frames. This creates a reference point, so that errors are not propagated through the entire video sequence.

H.264 uses more sophisticated motion compensation than older video encoding standards and contextadaptive binary arithmetic encoding. However, applying the DWT to H.264 may improve compression and image quality. In our research, we will apply many of the compression techniques used in JPEG2000 to the I frame of H.264 in order to improve compression and reduce low bitrate artifacts, such as blocking artifacts and color distortion. The two approaches can be compared using objective metrics, such as mean square error, or subjective metrics.

**Image Fusion: Increase of Depth-of-Field by Combination of Multiple Images**

Image fusion involves combining multiple images of one scene, where each image is obtained with a slightly different focal point. The objective is to produce a final image with a large depth-of-field and a high signal-to-noise ratio. This computational photography technique is useful in increasing the depth-of-field, without losing signal-to-noise ratio in low-light and macro/micro photography.

In traditional photography, image quality is subject to trade-offs under low-light situations. If a large depth-of-field is desired, the aperture must be closed substantially, resulting in a longer shutter-speed. Longer shutter-speeds often result in motion blur, so the sensor International Organization for Standardization (ISO) must be increased. This results in a noisier image. If a high signal-to-noise ratio is desired, the ISO must be set to the minimum. A low ISO requires more light, so the aperture must be opened, resulting in a small depth-of-field. Image fusion seeks to allow for a high signal-to-noise ratio, as well as a large depth-of-field.

In macro and micro photography, a large depth-of-field image is traditionally impossible, even if the aperture of the camera is almost completely closed. Image fusion seeks to produce high depth-of-field images in macro and micro photography.

Existing algorithms for image fusion fall into two categories, those that operate in the spatial domain and those that operate in the frequency domain. In both of these types of algorithms, a comparison is performed among the multiple images to select which image is sharpest at every pixel. In our research, we made various improvements to these algorithms.

One method involves using variable window sizes. Edge-detection is first performed on an initial decision map based on a large window size. Based on the distance from edges, a new window size is obtained at each pixel. Another method involves performing median-filtering on the decision map. Both techniques successfully reduce the mean square error of the resulting image by reducing noise in areas far from decision boundaries, without losing preciseness near decision boundaries.

This image fusion technique has potential applications in three-dimensional high-definition television. A potential approach for three-dimensional high-definition television is through depth-image-based rendering (DIBR), which requires a two-dimensional image and a per-pixel depth-map. Depth-image-based rendering allows for one way to incorporate multiple views and alternate camera-positions for three-dimensional high-definition television.
Quantum Information (RLE) -- Quantum computers and communication systems are devices that store and process information on quantum systems such as atoms, photons, superconducting systems, etc. Quantum information processing differs from classical information processing in that information is stored and processed in a way that preserves quantum coherence. The Quantum Information Group is investigating methods for constructing quantum computers and quantum communication systems using atomic physics, quantum optics, and superconducting systems. In addition, the group is investigating applications of quantum information processing including novel quantum algorithms and communication protocols.

Keck Foundation Center for Extreme Quantum Information Theory (xQIT)
What are the ultimate powers of quantum computers, quantum communications and quantum precision measurement systems? MIT's new $3.5 million W. M. Keck Foundation Center for Extreme Quantum Information Theory (xQIT) has been inaugurated with $1.63 million in funding from the Keck Foundation, as well as funding from MIT and other sponsors, to discover answers to these fundamental, yet still unsolved, questions.

The new center enables a major new push by MIT theorists in the international race to determine the ultimate capabilities of quantum information systems. Establishing these theoretical capabilities would be a step towards being able to exploit quantum effects for novel applications, including computers, communication networks and global positioning systems.

Over the last half century, the components of computers have gotten smaller by a factor of two every year and a half, the phenomenon known as Moore's law. In current computers, the smallest wires and transistors are coming close to a size of one hundred nanometers across, a thousand times the diameter of an atom. Quantum mechanics is the theory of physics that describes the behavior of matter and energy in extreme conditions such as short times and tiny distances. As transistors and wires become smaller and smaller, they inevitably begin to behave in intrinsically quantum mechanical ways.

Quantum computers store and process information at the level of individual quanta—atoms, photons, and electrons. Even if Moore's law persists, commercial quantum computers are not yet due on the shelves for another few decades; nonetheless, prototype quantum computers consisting of a small number of atoms and quantum communication systems that use single photons have been built and operated.

Researchers at the W.M. Keck Center for Extreme Quantum Information Theory (xQIT) are working to investigate the limits of computation and communication. We are working to uncover the abilities of quantum computers to solve hard problems. We are investigating the capacities of noisy quantum channels. We have shown how quantum channel capacity can be enhanced using entanglement. We have derived limits on the capacities of broadband quantum channels with and without entanglement assistance. Finally, we are investigating the ultimate physical limits to the accuracy of sensing and measurement. We are studying alternative approaches to quantum gravity based both on quantum limits to the measurement of space and time, and on emergent solid-state approaches.
Quantum Communication

The problem of maintaining the coherence of quantum information as it is moved from atoms to photons, transported through space, and moved back from photons to atoms, is a difficult one. Exactly because quantum information provides additional opportunities for storing and processing information, it also provides additional opportunities for errors, loss, and the corruption of that information. We are investigating the capacities of noisy quantum channels. We have shown how quantum channel capacity can be enhanced using entanglement. We have derived limits on the capacities of broadband quantum channels with and without entanglement assistance. Finally, we are investigating the ultimate physical limits to the accuracy of sensing and measurement.

xQIT: The Pressing Need for Advances in Extreme Quantum Information Theory

Over the last half century, the components of computers have gotten smaller by a factor of two every 18 months, a phenomenon known as Moore’s law. In state-of-the-art computers, the smallest wires and transistors are approaching 100 nm feature size, which is approximately 1000x the diameter of an atom. Quantum mechanics is the theory of physics that describes the behavior of matter and energy in extreme conditions, such as short times and tiny distances. As transistors and wires become smaller and smaller, they inevitably begin to behave in intrinsically quantum mechanical ways. Thus, whereas the quantum mechanics of semiconductor band theory has given us the microprocessors and laser diodes that have fueled our information age computers and communication systems, these technologies have not exhibited macroscopically quantum-mechanical effects. This will no longer be true as we drive forward to ever smaller and faster devices, and so it becomes essential to address information science in a fully quantum mechanical setting, viz., we need quantum computers and quantum communications.

Quantum computers and quantum communication systems operate at the level of individual quanta—atoms, photons, and electrons. They store, process, and transmit information at the smallest possible scales, and using the minimum possible energy. Even if Moore’s law persists, commercial quantum computers are not yet due on the shelves for another few decades; nonetheless, prototype quantum computers consisting of a small number of atoms and quantum communication systems that use single photons have been built and operated. Quantum mechanics is famously counterintuitive. (Einstein, despite making great contributions to quantum mechanics, never fully accepted it.) Quantum computers and communication systems exploit quantum weirdness to do things that classical information technologies cannot. A quantum computer could search databases and break codes that no classical computer could search or break. Quantum communication systems allow the creation of unbreakable codes, and could be used to teleport the state of matter from one place to another. Quantum enhancements to the Global Positioning System (GPS) could greatly enhance its accuracy.

What more could quantum computers and quantum communication systems do? Might quantum computers be able to solve harder problems than code breaking? Could quantum communication channels convey information at much higher rates than conventional radio frequency or optical communication channels? What are the ultimate attainable accuracies—based on the laws of physics—of measurement and sensing systems such as GPS? Despite much productive research into the theory of quantum computation and quantum communication, the answers to these questions are not known. The ultimate capabilities of quantum computers and quantum communication systems, pressed to their extremes, remain to be discovered. Our efforts to meet these challenges will focus on three areas:
xQIT: Fundamental Limits on Quantum Sensing and Control

The exponential advance in computing power embodied in Moore’s law arises out of the longstanding and ongoing miniaturization process whereby the transistors on computer chips become smaller and smaller and the chips themselves grow more complicated and powerful (and power hungry). Continuation of this miniaturization process requires ever more precise instrumentation and lithography techniques. As the components of computers press down to the quantum-mechanical scale, so, too, do the instruments used to construct those components.

The advance of computing power is just one example of the march of technologies towards the quantum scale. Other powerful technologies rely intrinsically on quantum technologies. Thus, for example, the Global Positioning System derives its astounding capability from atomic clocks whose accuracies are inherently limited by the laws of quantum mechanics. To construct more powerful computers and more accurate atomic clocks, and to continue the advance of quantum technologies in general, we must understand the fundamental physical limits to the processes of sensing, control, and measurement that are imposed by quantum mechanics.

The physical laws that govern how much information a measurement apparatus or sensor can obtain are closely related to the physics of quantum communication. As Shannon noted, when an apparatus obtains information about some system, the interaction between system and apparatus is essentially a noisy communication channel: the system effectively “sends” information to the measurement apparatus, and that information is corrupted by noise and distortion. Measurement and sensing are key components of the general problem of quantum control, in which information is obtained and fed back to drive a quantum system towards some desired state or dynamics.

Measurement, sensing, and control are fundamentally concerned with the gathering, processing, and application of information, so it should come as no surprise that quantum mechanics introduces new features to these procedures. In particular, measurement uncertainty is intrinsic to quantum mechanics. Thus, after all technical noises are eliminated, the fundamental limits to the accuracy of measurement devices and sensors are those posed by quantum mechanics. Just as in the case of computation and communication, however, state-of-the-art precision measurement systems—such as optical interferometers, including those used for lithography—are reaching quantum-limited performance. Once again, these are standard quantum limits associated with the specific architectures of, say, interferometry with laser light. But quantum mechanics also provides new ways in which systems can be configured to obtain, process, and apply information, and the capabilities of these techniques—which employ peculiar quantum effects such as squeezing or entanglement—are not bound by the standard quantum limits. For example, it has long been known that the quantum-limited performance of squeezed-state interferometry is far better than the standard quantum limit, and more recently it has been shown that entanglement offers similar performance gains for optical lithography.

The rapid miniaturization of computer circuitry over the past half century, embodied in Moore’s law, has given rise to huge advances in computational power. Moore’s law itself arose from the similarly rapid increase in the accuracy and precision of technologies for measurement, sensing, manufacturing, and control. What are the ultimate physical limits on this miniaturization progression? Just how accurate can measurements, sensors, and control systems become?
how can we use quantum mechanics to attain those limits of accuracy? Answering these questions is crucial to continuing Moore’s law to the atomic scale. As Feynman noted, “There’s plenty of room at the bottom.” The frontier of the very small is in fact a huge place—as long as one possesses the skills to live there. In attempting to reach the ultimate limits of accuracy for measurement, sensing, and control, we are developing the skills to explore and inhabit this frontier.

PROF. MURIEL MEDARD
Associate Professor of Electrical Engineering
Associate Director, Laboratory for Information and Decision Systems (LIDS)
http://web.mit.edu/medard/www/medard.html

Professor Médard’s research interests are in the areas of network coding and reliable communications, particularly for optical and wireless networks. The motivation of Professor Médard’s work is the fact that communications have moved away from point-to-point, or link, models, to networked models. Moreover, the nature of these networks is increasingly heterogeneous, relying on a federation of different physical layers, ranging from optical fiber communications to wireless links. This heterogeneity allows for flexibility and quasi-ubiquitous access to networked systems, but often at the expense of robustness and reliability. Growing societal reliance on networked services renders an interruption or degradation of service, whether by malicious attack or inherent variability of the physical layer, particularly grievous. I seek to determine, in Médard’s research, a means of providing effective and reliable networked communications, with strong consideration of the physical layer.

Optical Networks
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 backup 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.

Evolutionary Methods in Network Coding Applied to MANETs
While network coding has been shown to offer various advantages over traditional routing, in order to see network coding widely deployed in real networks, it still remains to show that the amount of overhead incurred by additional coding operations can be kept minimal and eventually outweighed by the benefits network coding provides.
Whereas most network coding solutions assume that the coding operations are performed at all nodes, we have pointed out in previous work that it is often possible to achieve the network coding advantage by coding only at a subset of nodes. Determining a minimal set of nodes where coding is required is NP-hard, as well as finding its close approximation. Thus, we have previously proposed evolutionary approaches toward a practical multicast protocol that achieves the full benefit of network coding in terms of throughput, while performing coding operations only when required at as few nodes as possible. Suppose that we have an ad hoc wireless network currently operating solely with traditional routing and wish to employ network coding on the network to achieve the maximal throughput promised by the network coding theory. However, for handling the mathematical operations required for coding, the network nodes that have to perform network coding may need some changes in their software and/or hardware, which would necessarily incur some additional cost. Therefore, a very interesting and also practically important question that may arise in such a situation is whether we should change the entire network for network coding or modifying only a subset of nodes would be enough. Along the same direction, many more interesting questions may follow: If only a small number of coding nodes are enough, as previously found in [1, 3] with a generic network model, where should those coding nodes be located? Can we fix their locations despite varying communication demands? How should those coding nodes interact with other non-coding nodes?

In recent work, we considered the multicast scenario in a heterogeneous ad hoc wireless network where a number of coding nodes are to be placed among the legacy nodes that do not handle network coding operations well, to which previously proposed evolutionary framework is applied to provide better understanding, if not complete answers, of the questions raised above. In particular, we have shown that the evolutionary approach is well generalized to the case of heterogeneous wireless networks with only slight changes in the fitness function and the backward evaluation phase, retaining its key advantages over existing centralized approaches [7, 8] in terms of the efficient operation through its spatially and temporally distributed structure and the superior performance in finding a minimal set of coding nodes.

Once a set of coding nodes is given, we can run the distributed algorithm directly over the network, during which each legacy node temporarily emulates coding operations on the application layer to find a minimal set of the legacy nodes that have to keep performing the emulated coding during the normal operation of the network to achieve the multicast capacity. More interestingly, we can utilize the evolutionary approach to investigate various issues regarding where and how to place coding nodes in heterogeneous wireless networks, which led to the following findings:

(*) To find out how many coding nodes are required to achieve the multicast capacity, we generated 100 random wireless topologies for each of 18 different parameter sets with either 20 or 40 nodes and the number of receivers varying from 4 to 10. We found that in most cases (over 90% for networks with 20 nodes and from 57% to 86% for networks with 40 nodes) network coding is not needed at all to achieve the multicast capacity. Even in the cases where network coding is needed, the number of coding nodes does not exceed 15% of the total number of nodes; the number of required coding nodes is at most 3 in networks with 20 nodes and 5 in those with 40 nodes. This suggests that, while it is necessary to assume network coding everywhere initially to calculate the multicast capacity, to actually achieve the calculated maximal throughput coding operations may not be needed at all, and even when needed, only at a very small subset of nodes, thus incurring very little amount of overhead.
(*) With a slight change in the fitness function, we have found that, for the coding nodes found above, it is often possible to find alternative nodes to perform coding operations to achieve the given multicast capacity. In other words, the location of the coding nodes can often be flexible rather than fixed for a specific traffic pattern, implying that the found coding nodes can be shared by different multicast requests.

(*) To verify the intuition of sharing coding nodes among different communication demands, we picked two representative topologies from those used in the first experiment, and for each topology we randomly generated another 30 multicast requests to find the locations of the coding nodes required for different traffic patterns. We found out that at least half of the coding nodes were in common with different communication demands for the both topologies. This indicates that placing coding nodes at the commonly found locations for a number of sampled traffic patterns may be a good strategy in practice.

(*) It is worth to point out that at the end of the iteration, the algorithm yields not only the set of the coding nodes, but also the relevant network code at each interior node, whether it indicates coding or routing. Therefore, the problem of interactions among coding and non-coding nodes is already dealt with implicitly within the framework of the algorithm, whether the algorithm is used to minimize the number of legacy nodes that have to emulate coding with the given set of coding nodes or to find the potential locations of the coding nodes. In addition, given the vulnerability of ad hoc wireless networks to various kinds of losses, we have shown that, thanks to its iterative nature, the algorithm can operate without much disruption even in the presence of a moderate level of packet erasures caused by various reasons. Furthermore, the algorithm may become even more robust by employing the temporally distributed structure in previous work, whose initial motivation was better utilization of computational resources over the network. We have shown that the temporally distributed structure also offers a significant advantage in overcoming the adverse effect of packet erasures on the performance of the algorithm.

**Information Theory for MANETs**

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

One of the effects of channel dynamics is that feedback can be used to adapt to changing conditions. Transmitter knowledge of channel state has a great impact on wideband fading channel capacity. However, in the low SNR regime, power per dimension does not suffice to provide an accurate measurement of the channel over the entire spectrum.

In the presence of feedback, we may collect information at the transmitter about some aspects of the channel quality over a certain portion of the spectrum. In this work, we investigate the effect of such information. With Professor Zheng and the student consider channel testing with a finite amount of energy over a block-fading channel in both time and frequency. We consider a transmission scheme in which the wideband channel is decomposed into many parallel narrowband subchannels, each used with a binary modulation scheme. The quality of each subchannel corresponds to the crossover probability of a binary symmetric channel. We use a multi-armed bandit approach to consider the relative costs and benefits of allotting energy for testing versus transmission, and for repeated testing a single subchannel versus testing different subchannels. We give both upper and lower bounds on the number of subchannels that should be probed for throughput maximization under the scheme we have chosen. Bounds are in terms of
available transmission energy, available bandwidth and fading characteristics of the channel. Moreover, in the numerical results, the two bounds are close.

Power efficiency is a capital issue in the study of mobile wireless nodes owing to constraints on their battery size and weight. In practice, especially for low-power nodes, it is often the case that the power consumed for non-transmission processes is not always negligible. With Professor Zheng and the student, we have considered the channels with a special form of overhead: a processing energy cost whenever a non-zero signal is transmitted. We have shown that under certain conditions, achieving the capacity of such channels requires intermittent, or ‘bursty’, transmissions. Thus, an optimal sleeping schedule can be specified for wireless nodes to achieve the optimal power efficiency. We have shown that in the low SNR regime, there is a simple relation between the optimal burstiness and the overhead cost: one should use a fraction of the available degrees of freedom at an SNR level of $(2e)^{1/2}$, where $e$ is the normalized overhead energy cost. We have extended this result to use bursty Gaussian transmissions in multiple parallel channels with different noise levels. The result can be intuitively interpreted as a “glue pouring” process, generalizing the well-known water pouring solution. We have used this approach to compute the achievable rate region of the multiple access channel with overhead cost.

The issue of delay in an information-theoretic setting has always been rendered difficult by the fact that traditional notions of capacity have no upper bound on delay. In order to quantify the delay benefits of coding in MANETs, we have investigated rateless codes with Professor Ozdaglar, Professor Eryilmaz (Ohio Sate University) and the student. In an unreliable packet network setting, we study the performance gains of optimal transmission strategies in the presence and absence of coding capability at the transmitter, where performance is measured in delay and throughput. Although the results apply to a large class of coding strategies including Maximum Distance Separable (MDS) and Digital Fountain codes, we use random network codes in the discussions because these codes have a greater applicability for complex network topologies. To that end, after introducing a key setting in which performance analysis and comparison can be carried out, we provide closed form as well as asymptotic expressions for the delay performance with and without network coding. We show that the network coding capability can lead to arbitrarily better delay performance as opposed to traditional strategies.

With Professor Ozdaglar, Professor Eryilmaz (Ohio State University) and the student, we have considered the problem of rate allocation in a fading Gaussian multiple-access channel with fixed transmission powers. The goal is to maximize a general concave utility function of the expected achieved rates of the users. There are different approaches to this problem in the literature. From an information theoretic point of view, rates are allocated only by using the channel state information. The queueing theory approach utilizes the global queue-length information for rate allocation to guarantee throughput optimality as well as maximizing a utility function of the rates. In this work, we have made a connection between these two approaches by showing that the information theoretic capacity region of a multiple-access channel and its stability region are equivalent. Moreover, the numerical results show that a simple greedy policy which does not use the queue-length information can outperform queue-length based policies in terms of convergence rate and fairness.

**Information-Theoretic Aspects of Network Coding**

We have considered, with Professor Shah and Professor Koetter from TUM and our student, the problem of serving multicast flows in a crossbar switch is considered. We have shown linear network coding across packets of a flow can achieve a larger rate region compared to the nocoding
case. In addition to such throughput gains, the characterization of the rate region becomes simpler when coding is allowed. We have characterized the rate region with coding graph theoretically, in terms of the stable set polytope of the “enhanced conflict graph” of the traffic pattern. No such graph theoretic characterization of the rate region is known for the case of fanout splitting without coding. The minimum speedup needed to achieve 100% throughput with coding we have shown to be upper bounded by the imperfection ratio of the enhanced conflict graph. In particular, we have applied this result to K x N switches with traffic patterns consisting of unicasts and broadcasts only and an upper bound is obtained on the speedup. Such bounds show that in multicast switches, speedup, which is usually implemented in hardware, can often be substituted by network coding, which can be done in software. We have shown that computing an offline schedule (using prior knowledge of the flow arrival rates) can be reduced to certain graph coloring problems. We have also proposed a graph-theoretic online scheduling algorithm (using only current queue occupancy information), that stabilizes the queues for all rates.

Joint Source and Network Coding
This work explored robust and scalable approaches to the reach-back problem for extracting data from several distributed sources. The approach will sought to establish a parallelizable and distributed approach to pull data from correlated sources under a possibly unknown and varying network topology. We considered network topology changes that are too slow to allow for averaging approaches, such as traditional coding to achieve mean performance for ergodic systems, but too rapid to allow for off-line architectural changes. These changes in topology are congruent with the slow but dramatic changes in topology associated with satellite systems, for instance because of coverage issues. We have also considered joint routing and compression in a topology-independent fashion. In particular, approaches that do not require updating of routing information, which, because of the long delays associated with satellite systems, may severely hamper the operation of traditional networking approaches. Instead, the work uses a distributed approach in which each node performs a mapping from inputs to outputs in a fashion that blurs the line between routing and compression. This distributed approach would require no or little sharing of states among nodes or even overall knowledge of topology. Instead, the net effect of transmission through the network need only be known at the receiving nodes. The obviation of the need to share state among nodes implies that stability issues under network changes are significantly alleviated. Such work begins to address meta data integration of disparate information (something like a web search engine that examines meta data on disparate sources and is able to associate the data to add value in an information sense).

Practical Approaches to Wireless Network Coding
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 the 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.

Network coding has been shown to improve throughput and reliability in a variety of theoretical and practical settings. But it has had limited success in areas like sensor networks due to its two limitations. First, network codes are “all-or-nothing” codes; the sink cannot decode any information unless it receives as many coded packets as the original number of packets. Second, sensor networks often measure physical signals which show a high degree of spatial correlation; present network coding techniques cannot perform in-network lossy compression to take
advantage of the spatial correlation. With Professor Katabi, Professor Jaggu (Chinese University of Hong Kong) and students, we have presented “Real” Network Codes that are linear over real fields. We build on recent results from Compressed Sensing to develop new codes which can be decoded to get progressively more accurate approximations as more coded packets are received at the sink. Further, they can compress distributed correlated data inside the network without requiring that the nodes know how the data is correlated. Thus, Real Network Codes combine two exciting but hitherto separate areas, Network Coding and Compressed Sensing, allowing them to keep the advantages of network coding, but also make them capable of finding low distortion approximations with partial information and perform distributed compression of correlated data.

We have furthered consideration of the interplay of the physical layer and network coding by considering symbol-level network coding. With Professor Katabi, her student and Professor Balakrishnan, we have introduced FUSE, a system that improves the throughput of wireless mesh networks. FUSE exploits a basic property of mesh networks: even when no node receives a packet correctly, any given bit is likely to be received by some node correctly. Instead of insisting on receiving correct packets, FUSE routers use physical layer hints to make their best guess about which bits in a corrupted packet are likely to be correct and forward them to the destination. Even though this approach inevitably lets erroneous bits through, we find that it can achieve high throughput without compromising end-to-end reliability. The core component of FUSE is a novel network code that operates on small groups of bits, called symbols. It allows the nodes to opportunistically route groups of bits to their destination with low overhead. FUSE’s network code also incorporates an end-to-end error correction component that the destination uses to correct any errors that might seep through. We have implemented FUSE on a software radio platform running the Zigbee radio protocol. Experiments on a 25-node indoor testbed show that FUSE has a throughput gain of a factor of 2.8 over MORE, a state-of-the-art opportunistic routing scheme, and about 3.9 times over traditional routing using the ETX metric.

The overhearing of transmissions that is inherent in wireless communications has generally been considered as a deleterious effect, leading to interference. With Professor Katabi, Professor Crowcroft (University of Cambridge) and their students, we have proposed COPE, a new architecture for wireless mesh networks. In addition to forwarding packets, routers mix (i.e., code) packets from different sources to increase the information content of each transmission. We show that intelligently mixing packets increases network throughput. The design is rooted in the theory of network coding. Prior work on network coding is mainly theoretical and focuses on multicast traffic. This paper aims to bridge theory with practice; it addresses the common case of unicast traffic, dynamic and potentially bursty flows, and practical issues facing the integration of network coding in the current network stack. We evaluate the design on a 20-node wireless network, and discuss the results of the first testbed deployment of wireless network coding. The results show that using COPE at the forwarding layer, without modifying routing and higher layers, increases network throughput. The gains vary from a few percent to several folds depending on the traffic pattern, congestion level, and transport protocol.

The variability of MANETs entails considerable difficulties in reacting to changing conditions and also in acquiring global information about the network. The problem of establishing minimumcost multicast connections in coded networks can be viewed as an optimization problem, and decentralized algorithms were proposed by Lun et al. to compute the optimal subgraph using the subgradient method on the dual problem. However, the convergence rate problem for these algorithms remains open. There are limited results in the literature on the
convergence rate of the subgradient method in the dual space, but the convergence rate of the primal solutions was not known. With Professor Ozdaglar and the student, we have analyzed the convergence rates of the min-cost subgraph algorithms in both the dual and the primal spaces. We have shown that using the incremental subgradient method on the dual problem with appropriately chosen step sizes yields linear convergence rate to a neighborhood of the optimal solution. Also, if we use constant step sizes in the subgradient method and simple averaging for primal recovery, the primal solutions recovered from the dual iterations converge to a neighborhood of the optimal solution with rate $O(1/n)$.

Another important aspect of wireless communications is latency, particularly in acoustic channels or channels over long distances such as satellite channels. With Dr. Stojanovic and a student, we have considered underwater acoustic channels. The goal of this research is two-fold. First, to establish a tractable model for the underwater acoustic channel useful for network optimization in terms of convexity. Second, to propose a network coding based lower bound for transmission power in underwater acoustic networks, and compare this bound to the performance of several network layer schemes. The underwater acoustic channel is characterized by a path loss that depends strongly on transmission distance and signal frequency. The exact relationship among power, transmission band, distance and capacity for the Gaussian noise scenario is a complicated one. We have provided a closed-form approximate model for (1) transmission power and (2) optimal frequency band to use, as functions of distance and capacity. The model is obtained through numerical evaluation of analytical results that take into account physical models of acoustic propagation loss and ambient noise. We have applied network coding to determine a lower bound to transmission power for a multicast scenario, for a variety of multicast data rates and transmission distances of interest for practical systems, exploiting physical properties of the underwater acoustic channel. The results quantify the performance gap in transmission power between a variety of routing and network coding schemes and the network coding based lower bound. We illustrate results numerically for different network scenarios.

Security Aspects of Network Coding

Network coding substantially increases network throughput. But since it involves mixing of information inside the network, a single corrupted packet generated by a malicious node can end up contaminating all the information reaching a destination, preventing decoding. With Professors Jaggi (Chinese University of Hong Kong), Katabi, Effros (Caltech), Langberg (Open University of Israel) and the students, we have introduced distributed polynomial-time rate-optimal network codes that work in the presence of Byzantine nodes. We have developed algorithms that target adversaries with different attacking capabilities. When the adversary can eavesdrop on all links and jam $z$ links, the first algorithm achieves a rate of $C \geq 2z$, where $C$ is the network capacity. In contrast, when the adversary has limited eavesdropping capabilities, we provide algorithms that achieve the higher rate of $C \geq z$. The algorithms attain the optimal rate given the strength of the adversary. They are information theoretically secure. They operate in a distributed manner, assume no knowledge of the topology, and can be designed and implemented in polynomial-time. Furthermore, only the source and destination need to be modified; non-malicious nodes inside the network are oblivious to the presence of adversaries and implement a classical distributed network code. Finally, the algorithms work over wired and wireless network.

Network coding can also be used to enhance cryptographic approaches. With Professor Barros (University of Porto) and his students, we have considered the issue of confidentiality in multicast network coding, by assuming that the encoding matrices, based upon variants of random linear network coding, are given only to the source and sinks. Based on this assumption, we provide a
characterization of the mutual information between the encoded data and the two elements that can lead to information disclosure: the matrices of random coefficients and, naturally, the original data itself. The results, some of which hold even with finite block lengths, show that, predicated on optimal source-coding, information-theoretic security is achievable for any field size without loss in terms of decoding probability. It follows that protecting the encoding matrix is generally sufficient to ensure confidentiality of network coded data.

The issue of security in network coding is particularly important when it is used in peer-to-peer networking. Using network coding, a peer node can reconstruct the whole file when it has received enough degrees of freedom to decode all the blocks. This scheme is completely distributed, and eliminates the need for a scheduler, as any block transmitted contains partial information of all the blocks that the sender possesses. It has been shown both mathematically and through live trials that the random linear coding scheme significantly reduces the downloading time and improves the robustness of the system.

A major concern for any network coding system is the protection against malicious nodes. Take the above content distribution system for example. If a node in the P2P network behaves maliciously, it can create a polluted block with valid coding coefficients, and then sends it out. Here, coding coefficients refer to the random linear coefficients used to generate this block. If there is no mechanism for a peer to check the integrity of a received block, a receiver of this polluted block would not be able to decode anything for the file at all, even if all the other blocks it has received are valid.

To make things worse, the receiver would mix this polluted block with other blocks and send them out to other peers, and the pollution can quickly propagate to the whole network. This makes coding based content distribution even more vulnerable than the traditional P2P networks, and several attempts were made to address this problem. Some previous work proposed to use homomorphic hash functions in content distribution systems to detect polluted packets, or the suggested the use of a Secure Random Checksum (SRC) which requires less computation than the homomorphic hash function. However, one requires a secure channel to transmit the SRCs to all the nodes in the network. Work from Microsoft proposed a signature scheme based on Weil pairing on elliptic curves and provides authentication of the data in addition to pollution detection, but the computation complexity of this solution is quite high. Moreover, the security offered by elliptic curves that admit Weil pairing is still a topic of debate in the scientific community. In collaboration with Dr. Han (AFRL), Dr. Kaljer (HP Research Labs) and my student, we have developed a homomorphic signature scheme that is not based on elliptic curves, and is designed specifically for random linear coded systems. We view all blocks of the file as vectors, and make use of the fact that all valid vectors transmitted in the network should belong to the subspace spanned by the original set of vectors from the file. The scheme can be used to easily check the membership of a received vector in the given subspace, and at the same time, it is hard for a node to generate a vector that is not in that subspace but passes the signature test. We have shown that this signature scheme is secure, insofar as it reduces to the Diffie-Hellman problem, and that the overhead for the scheme is negligible for large files.

The discussion above indicates that there are different approaches to using network coding in security. An important question that emerges is how to guide the choice of approaches. With Professor Barros (University of Porto) and my student, we have studied the transmission overhead associated with three different schemes for detecting Byzantine adversaries at a node using network coding: end-to-end error correction, packet-based Byzantine detection scheme,
and generation-based Byzantine detection scheme. In end-to-end error correction, it is known that we can correct up to the min-cut between the source and destinations. However, if we use Byzantine detection schemes, we can detect polluted data, drop them, and therefore, only transmit valid data. For the dropped data, the destinations perform erasure correction, which is computationally lighter than error correction. We show that, with enough attackers present in the network, Byzantine detection schemes may improve the throughput of the network since we choose to forward only reliable information. When the probability of attack is high, a packet-based detection scheme is the most bandwidth efficient; however, when the probability of attack is low, the overhead involved with signing each packet becomes costly, and the generation-based scheme may be preferred. Finally, we characterize the tradeoff between generation size and overhead of detection in bits as the probability of attack increases in the network.

**DR. UNA-MAY O’REILLY**  
Principal Research Scientist  
Emergent Design Group, Computer Science and Artificial Intelligence Laboratory  
http://people.csail.mit.edu/unamay/  
http://www.csail.mit.edu/user/824

Dr. O’Reilly is active in the field of evolutionary computation, specifically investigating the theory, analysis and application of genetic programming. Her theoretical and analytic work spans schema theory, comparison with other stochastic search techniques and population sizing models. With colleagues, she has applied genetic programming to compiler optimization and creative architectural design. She is lead editor of the forthcoming book “Genetic Programming Theory and Practice, II”.

**Evolutionary Design and Optimization Group (EVO-DesignOpt)**

The unrelenting growth of complexity, data creation and tighter performance deadlines has given rise to problems that are unyielding to statistical or kernel-based machine learning techniques, convex optimization or evolutionary algorithms alone. However, a combination of these techniques can yield powerful algorithms and solutions.

EVO-DesignOpt explores efficient ways to combine different techniques to solve hard optimization and design problems in domains of high complexity.

The techniques we develop can address problems related to:

(*) efficient exploitation of multicore processors  
(*) parallel high-performance computing  
(*) networks (communication, management)  
(*) circuits (sizing, MOSFET modeling, IC-CAD)  
(*) embedded systems (control, mapping)  
(*) computer systems (compilers, run-time and operating scheduling and resource allocation)  
(*) complex challenges such as transportation management, logistics, energy efficiency, and surveillance  
(*) other domains with complex characteristics and specifications

FOCUS is on evolutionary algorithms for optimization, machine learning and adaptive systems.
The techniques have various sweet spots:

(1) Typically Known
(*) they determine "good enough" solutions in the class of NP-hard or NP-complete problems
(*) they optimize without needing gradient information or analytic functions
(*) they naturally parallelize
(*) they easily incorporate and leverage expert knowledge of the problem domain

(2) Less Heard Of
(*) they solve machine learning problems by recasting them as search problems
(*) they learn model structure as well as parameters (Genetic Programming)
(*) they solve distributed problems requiring heterogenous or homogenous sub-solutions
(*) they are naturally robust for soft computing

Genetic Algorithms for Network Coding
Minimization of resources required for network coding is an NP-hard problem. We have designed scalable genetic algorithms to solve the problem for the multi-cast scenario. The NWC-GA incorporates network topological knowledge in its representation and adaptive operators.

We have developed a NWC-GA for a distributed network and the multiple-unicast scenario that is embedded spatially (on the network being coded) and temporally. (see GECCO 2007 publication)

We have developed a Multi-objective GA that provides pareto-front tradeoff options between coding and link costs. (see MILCOMM 2007 publication)

To achieve practical network coding, we are addressing resource and throughput tradeoffs in additional multi and unicast scenarios.

Network coding is an alternative to conventional network routing.

An Evolutionary Approach to Network Coding Problems
Network coding is a novel technique that generalizes routing. In traditional routing, each interior network node simply forwards the received data or sends out multiple copies of it. In contrast, network coding allows interior network nodes to perform arbitrary mathematical operations, e.g., summation or subtraction, to combine the data received from different links. While most network coding solutions employ coding at all possible nodes, it is often possible to achieve the network coding advantage by coding only at a subset of nodes.

If network coding is handled at the application layer, we can minimize the cost of network coding by identifying the nodes where access up to the application layer is not necessary. If network coding is integrated in the buffer management of a router, it is important to understand where and how many such special routers must be deployed to satisfy the communication demands.

Determining a minimal set of nodes where coding is required is difficult. The optimization problem to find the minimal number of required coding nodes, or even its crude approximation, is NP-hard. The structure of the problem is very little known for the application of traditional optimization methods, and no further methods have been proposed thus far beyond centralized greedy algorithms or LP formulations with an exponential number of variables/constraints.
For the multicast scenario with a single source and a set of receiver nodes, with the constraint of the target multicast throughput to achieve, we seek to find a method to yield sufficiently good solutions, i.e., at least as good as those obtained by the existing centralized algorithms, in an efficient and practicable manner.

How?

We propose an evolutionary approach, based on a genetic algorithm, with a number of novel mechanisms which greatly improve the algorithm’s performance and practicability. We first develop a block-wise genotype encoding with the associated genetic operators which, by preserving the inherent modularity between the variables given by the network topology, is shown to often lead to far superior solutions than those obtained by existing algorithms. Despite its stochastic nature, the proposed algorithm provides the worst-case performance bound at least as good as the existing algorithms.

Our proposed algorithm operates in a distributed fashion, offering a significantly lower complexity compared with the existing centralized algorithms. Combined with a decentralized network coding framework, the algorithm enables a distributed network coding protocol where the resources used for coding are optimized on the fly in a setup phase. In addition, we develop a novel framework of the temporally distributed genetic algorithm, which in the experiments leads to a substantial gain in terms of the time to convergence, as well as the benefit of robustness operation against delays, failures, or topological changes in the network.

Ongoing research topics include extending the proposed algorithm to investigate the tradeoff between the coding and link costs for multicast network coding and applying evolutionary algorithms to the more generalized scenario of non-multicast network coding.

**PROF. JEFFREY H SHAPIRO**

Julius A Stratton Professor of Electrical Engineering
Director, Research Laboratory of Electronics (RLE)
Principal Investigator, Optical and Quantum Communications Group (RLE)
http://www.rle.mit.edu/rleonline/People/JeffreyH.Shapiro.html
http://www.rle.mit.edu/qoptics/

Dr. Shapiro’s research interests have centered on the application of communication theory to optical systems. He is best known for his work on the generation, detection, and application of squeezed-state light beams, but he has also published extensively in the areas of atmospheric optical communication and coherent laser radar.

**Quantum Information Technology: Entanglement, Teleportation and Quantum Memory**

Quantum superposition and quantum entanglement are the bedrock on which new theoretical paradigms for information transmission, storage, and processing are being built. The preeminent obstacle to the development of quantum information technology is the difficulty of transmitting quantum information over noisy and lossy quantum communication channels, recovering and refreshing the quantum information that is received, and then storing it in a reliable quantum memory.
With support from the Multidisciplinary Research Program of the University Research Initiative (MURI), we have assembled an interdisciplinary team from researchers at MIT and Northwestern University to overcome this obstacle. The focus of our program is an architecture we have established for long-distance, high-fidelity qubit teleportation. Its key elements are: (1) ultrabright, narrowband sources of polarization-entangled photon pairs; (2) long-distance transmission of entangled photons over standard telecom fiber; and (3) qubit storage and processing in trapped atom quantum memories.

The preeminent obstacle to the development of quantum information technology is the difficulty of transmitting quantum information over noisy and lossy quantum communication channels, recovering and refreshing the quantum information that is received, and then storing it in a reliable quantum memory. Under U.S. Army Research Office Grant DAAD19-00-1-0177, “Quantum Information Technology: Entanglement, Teleportation, and Quantum Memory,” a team of researchers from the Massachusetts Institute of Technology (MIT) and Northwestern University (NU) have undertaken a Multidisciplinary University Research Initiative (MURI) program to overcome this obstacle. In particular:

(*) We have developed an architecture for long-distance, high-fidelity qubit teleportation that uses a novel ultrabright narrowband source of polarization-entangled photon pairs, and a trapped-atom quantum memory whose loading can be verified nondestructively and whose structure permits all four Bell-state measurements to be performed.

(*) We are working to realize all the technology elements to instantiate our quantum communication architecture, including polarization entanglement sources based on parametric amplifiers or fiber Sagnac loops, long-distance entanglement distribution over standard telecom fiber and qubit storage and processing in trapped Rb-atom quantum memories.

(*) We are working on a variety of new concepts for quantum communication and memory that should greatly increase the likelihood that quantum information technology will have a practical future.

An overview of the MIT/NU program was presented by Professor Shapiro, the program’s Principal Investigator. The central thrust of the MIT portion of the program is a singlet-state architecture for long-distance, high-fidelity teleportation. Its essential components, conceived and to be developed by members of the MURI team are: an ultrabright narrowband source of polarization-entangled photon pairs, a trapped-atom quantum memory (PDF), and an architecture for connecting these source and memory elements via standard telecommunication fiber. The second major thrust area for the MIT/NU MURI program is the development of quadrature-based teleportation using a fiber-optic entanglement source. Additional efforts, under this program, will be devoted to a variety of theoretical problems related to the applications of entanglement and quantum communication.

The MIT/NU MURI program underwent a full-day review in October 2002, during its third year of existence. In going forward from that review, the MURI effort was refocused on its core agenda, i.e., technology development and supporting theory for long-distance, high-fidelity qubit teleportation.
**xQIT: Capacities and Coding for Quantum Communication Channels**

The ability to communicate is one of mankind’s most valuable and important abilities, and the growth of modern communication networks is one of today’s most enabling technologies. Simply stated, the world is "wired for comm," with its interconnected web of fiber optics, cellular wireless, and satellite communications linking people, computers, and a host of embedded processors in a myriad of ways that defy easy enumeration. Increasingly, technological and social progress hinges on the availability of high-quality communications.

Shannon’s theory for the capacity of classical communication channels was one of the most powerful and practical results in applied mathematics of the twentieth century. Shannon derived simple formulae for the amount of information that could be encoded, sent down noisy communication channels, and reliably decoded at the the far end. When it was published it turned conventional thinking -- which held that noise presented an unavoidable and impossible to defeat impediment to error-free communication -- upside down. Shannon taught us -- what is now so ingrained in our thinking as to be obvious— that with digital communication and appropriate error-control coding the presence of noise on a communication link restricts the maximum rate at which error-free communication can occur. This maximum rate, of course, is Shannon’s channel capacity. Because of the importance of its applications, Shannon’s theory has proven to be one of the most useful pieces of applied mathematics ever created. It represents a high point of applied mathematics in the twentieth century.

All communication channels, at bottom, are quantum mechanical. Existing fiberoptic communication channels, and initial demonstrations of satellite-based optical communications, are approaching performance limits set by quantum mechanics. Once again, these are called standard quantum limits, because these conventional communication systems were not designed to fully explore and exploit the possibilities offered by quantum physics. In fact, the ultimate limits on reliable classical information transmission over quantum channels are not understood, because the quantum version of Shannon’s theory is not yet fully established. Thus, despite recent advances (many by researchers at MIT) in deriving capacity bounds for quantum channels and in devising coding schemes for approaching ultimate communication-performance limits, the full capacity of the noisy quantum communication channel has yet to be determined.

**PROF. CHARLES G. SODINI**
Clarence J LeBel Professor in Electrical Engineering
http://www-mtl.mit.edu/researchgroups/sodini/
http://web.mit.edu/ipc/people/faculty/sodini.html

Professor Sodini’s principal fields of interest are electronics and integrated circuit design and technology. More specifically, his research concerns technology intensive integrated circuit and systems design, with application toward sensory interface electronics and wireless communication emphasizing analog signal processing and RF integrated circuits. He has served as President of the IEEE Solid-State Circuit Society.

**Coding in Wideband OFDM Wireless Communications with Adaptive Modulation**

To achieve high-speed wireless communications, such as streaming of next-generation Gigabit Internet or HDTV, orthogonal frequency division multiplexing (OFDM) has been proven as the enabling technology. In an indoor environment where reflections from the surrounding objects result in multiple copies of the transmitted signal arriving at the receiver, the channel is highly
frequency-selective over a wide bandwidth. An OFDM system decomposes such a channel into multiple flat fading sub-bands by transmitting the high data-rate signal in multiple parallel lower data-rate blocks. Furthermore, an OFDM system can exploit this channel characteristic to maximize the data rate by adapting the modulation per bin based on the estimated Signal-to-Noise Ratio (SNR). In addition, channel coding is necessary to achieve the required system performance with a limited transmit power. In this work, we determine suitable codes in an adaptive modulation OFDM system to achieve highest throughput with a constrained latency. In particular, we analyze the benefits and tradeoffs of such codes as convolutional coding, trellis-coded modulation, and capacity-approaching low-density parity-check codes used in current OFDM systems.

To measure the performance gain from coding with adaptive modulation in an indoor wireless environment, we have implemented a transceiver prototype. In this prototype, the adaptive modulation takes place in three steps. In step 1, the transmitter sends a training sequence, and the receiver measures the SNR on each bin. If the true SNR is known for each sub-band, the most efficient sub-band modulation that yields an uncoded bit error rate (BER) smaller than 10^-3 is selected. However, the errors in the estimation of channel and time and frequency synchronizations result in a loss in SNR that increases the SNR thresholds. Next, in step 2, the receiver feeds back to the transmitter the assigned modulation scheme, which the transmitter uses to sends the data packet in step 3.

Power Amplifier Design for Millimeter-Wave Imaging

This research investigates the challenges of designing a power amplifier (PA) that could be used in a millimeter-wave (MMW) imaging system. A 130-nm SiGe BiCMOS process was used to develop an understanding of the specification limits. At MMW frequencies, the operating frequencies are pushing towards the fT (200 GHz) of the devices. Furthermore, the low breakdown voltage of the bipolar devices limits the voltage swing and output power of the PA. To overcome this, a cascode topology was used in which the DC base resistance of the cascode transistor was reduced to increase the breakdown voltage of the transistor and allow more voltage swing. The reduced Miller effect from the cascode gave an increase in power gain.

A simulation study was conducted to determine the device parameters that limited the performance of MMW PAs. The operating frequency was pushed to 120 GHz, and a nominal PA was designed and simulated. Parameters within the model file were systematically changed, and the nominal PA was redesigned to compensate for the adjusted parameters. The change in performance could be attributed to the specific parameter. We found that the most significant parameters were the intrinsic and extrinsic base-collector capacitances rather than the base transit time. This showed that reducing the line widths of the bipolar devices provides greater gains in PA performance than reducing the base widths.

A test chip was submitted for fabrication in December 2006. Due to limitations of available test equipment, the operating frequency was reduced to 110 GHz. Using a 2-stage cascode design, the PA achieves a simulated maximum output power of 10.7 dBm and 6.7 dBm 1-dB compression point. The maximum power added efficiency is 5.1%, and it has a 13.6 dB power gain. It shows a maximum output power of 12 dBm and an 8.1 dBm 1-dB compression point. The maximum power added efficiency is 6.0%, and it has a 15-dB power gain at 77 GHz.
PROF. JOHN R WILLIAMS
Associate Professor of Civil and Environmental Engineering and Engineering Systems
Director, Auto-ID Labs
http://cee.mit.edu/williams
http://esd.mit.edu/Faculty_Pages/williams/williams.htm

In the Williams lab, the goal is to develop leading-edge computation and information technologies. These technologies will improve our ability to address complex scientific and engineering problems using large-scale simulation. Two main areas of that the lab focuses on are (1) simulation of particle systems and (2) information systems, particularly for online education.

The Internet of Things

The MIT Auto-ID Laboratory is dedicated to creating the Internet of Things using RFID and Wireless Sensor Networks. Our aim from the start was to create a global system for tracking goods using a single numbering system called the Electronic Product Code. The Auto-ID Labs are the leading global network of academic research laboratories in the field of networked RFID. The labs comprise seven of the world’s most renowned research universities located on four different continents.

PROF. MOE Z. WIN
Associate Professor of Aeronautics and Astronautics
http://web.mit.edu/aeroastro/people/win.html

Moe Win is an Associate Professor at the MIT Laboratory for Information & Decision Systems (LIDS). Prior to joining LIDS, he spent 5 years at AT&T Research Laboratories and 7 years at the Jet Propulsion Laboratory. His main research interests are the application of mathematical and statistical theories to communication, detection, and estimation problems. Specific current research topics include measurement and modeling of time-varying channels, design and analysis of multiple antenna systems, ultra-wide bandwidth (UWB) communications systems, optical communications systems, and space communications systems.

Dr. Win developed a wideband wireless experimentation facility under the Laboratory for Information and Decision Systems (LIDS) at MIT. The facility includes a unique automated high-precision measurement apparatus that has the ability to systematically measure and model wideband (in excess of several GHz) communication channels over time and space.

Wireless Communication and Network Sciences Laboratory

The main research interests are the applications of mathematical and statistical theories to communication, detection, and estimation problems. General research topics include location-aware networks, measurement and modeling of time-varying channels, design and analysis of multiple antenna systems, ultra-wide bandwidth (UWB) systems, optical transmission systems, and space communications systems. It is our firm belief that theory should be always complemented by experiments, and we have an ongoing commitment to the development of a state-of-the-art experimental facility. In brief, our research combines

(1) theoretical analysis for determination of fundamental performance limits;

(2) the design of practical algorithms that approach such ultimate limits; and
(3) experimentation, both for validation and for developing realistic statistical models.

**Cooperative and Distributed Techniques**

Cooperative processing constitutes a new networking paradigm whereby nodes work together in order to achieve a common goal. Harnessing the collective power of the network enables increased coverage, longer network life, and massively parallel processing. Specific contributions include:

(a) Outage-Optimal Opportunistic Relaying: Put forth simple opportunistic relaying strategies under an aggregate power constraint. Developed a distributed relay-selection algorithms requiring only local channel knowledge. Proved that opportunistic decode-and-forward relaying is outage-optimal, that is, it is equivalent in outage behavior to the optimal strategy that employs all potential relays. The results revealed that cooperation offers diversity benefits even when cooperative relays choose not to transmit but rather choose to cooperatively listen.

(b) Cooperation in Bandwidth-Constrained Wireless Sensor Networks: Evaluated two different fusion architectures in terms of system reliability and average energy consumption where the degree of cooperation among the sensor nodes varies. Proposed a consensus flooding protocol for cooperation. Obtained insights into the trade-offs between reliability and energy efficiency with regard to spatially varying sensor observations, network connectivity, and realistic link models.

(c) Optimal and Robust Power Allocation in Wireless Relay Channels: Developed an analytical framework to obtain the optimal relay power allocation in multiple-relay amplify-and-forward channels in the presence of ideal global channel state information (CSI). Proposed an efficient algorithm for relay power allocation using second-order conic programming. Extended the results to the case of non-ideal global CSI, and designed robust relay power allocation protocols using the worst-case approach.

(d) Detection in Censoring Sensor Networks: Established a general framework for decentralized binary hypothesis testing in which sensors are allowed to be cooperatively censored (put to `sleep') based on observed side-information. Studied the tradeoff between detection performance and resource consumption. Developed an asymptotically optimal strategy that is simple, distributed, and depends only on the local information, provided that the network has a large number of sensors and the false alarm probability is constrained to be small.

(e) Detection in Tree Networks with Bounded Height: Studied the detection performance of bounded height tree architectures for energy efficiency and bounded delay. Showed the surprising fact that under some mild conditions, the asymptotically optimal Neyman-Pearson detection performance of such an architecture is the same as the standard parallel configuration. Quantified the performance loss as a function of tree height for the Bayesian framework.

**Cooperative Localization for UWB Networks**

UWB technology is well-suited for localization due to its potential for highly accurate ranging and robust communication. Contributions include:

(1) Fundamental Performance Bounds: Proposed the notion of equivalent Fisher information (EFI) to characterize the localization accuracy. This decomposes the contributions from LOS,
NLOS, and a priori knowledge to position error bounds, resulting in new insights in node placement strategies.

(2) Scalable and Distributed Iterative Algorithms: Developed a scalable, cooperative distributed localization algorithm for large UWB networks, based on factor graphs and belief propagation.

**Interference Analysis in Heterogeneous Network**

Developed a mathematical model for coexistence analysis in wireless networks composed of both narrowband (NB) and UWB nodes. Work accounts for the spatial distribution of interferers, and the propagation characteristics of the wireless environment. Specific contributions include:

(1) Probabilistic Invariance of Aggregate Interference with Application to FCC Rule Making: Proved that cumulative interference from radiators located at points of a Poisson random set obeys stable laws and possesses a surprising invariance with respect to essentially any fading distribution. Hence, these results are valid for a large class of fading environments and are helpful in characterizing the effect of unlicensed transmitters in the context of rule making by the FCC in the US and equivalent regulatory agencies in Europe and Asia-Pacific.

(2) Spectral Outage: Characterized the spectrum of the aggregate interference at any location in the Poisson plane, and put forth the new concept of spectral outage probability (SOP). The SOP can be used to quantify and limit the impact of network interference on a given frequency band, and serves as an insightful network design criterion.

(3) Error and Capacity Performance: Derived the performance expressions (in terms of error probability and channel capacity) for a NB/UWB link subject to cumulative UWB/NB interference, fading, and additive white Gaussian noise (AWGN). Work generalizes the conventional analysis of linear detection in the presence of AWGN and fast fading, allowing the traditional results to be extended to include the effect of aggregate interference.

**Optimal Search Strategies**

Established a framework and determined the fundamental limits of search strategies by bringing together ideas from the disciplines of engineering and mathematics, involving communication, signal processing, convexity, and optimization theories. Specific contributions include:

(1) n-optimal Search: Developed methodologies for the design of deterministic search that approach the fundamental limits.

(2) Randomized Search: Proposed and analyzed a search strategy that is robust to variation in channel.

This work is applicable to a broad class of search scenarios including minimal-time search algorithms that exploit multipath for acquisition of wide bandwidth wireless signals. In particular, it provides the fundamental basis for the design and analysis of UWB fast synchronization systems, which are essential for the rapid deployment and operation of future communication and sensor networks.
Quantum Error Recovery
Quantum error correction efforts to date have generally focused on generic noise models, and thus generic error recovery procedures. Our contributions have examined the benefits of quantum error recovery (QER) tailored to a specific noise model. Specific contributions include:

(1) Optimum QER as a Semidefinite Program: Demonstrated that using entanglement fidelity as the measure of performance, the optimum QER operation can be computed as the result of a semidefinite program (SDP). An SDP is a convex optimization routine, for which efficient algorithms are well understood. In this way, for any given noise model and encoding, the optimum recovery can be computed.

(2) Eigen Analysis for QER: Demonstrated the utility of eigen-analysis in interpreting and deriving QER techniques. Developed an eigenvector based algorithm to approximate the optimum QER operation for high dimensional channels (for which computing the optimum via a SDP is computationally burdensome).

Subset Diversity Techniques
Subset diversity techniques are reduced-complexity diversity methods where only a subset of the available diversity branches are utilized. These techniques are applicable to the many different forms in which diversity arises. Our contributions have focused on spatial diversity through multiple antennas or relays; and multipath diversity due to wideband transmission. Specific contributions include:

(a) MIMO Systems: Developed an analytical framework for the performance of MIMO systems operating in multipath-fading environments, where a subset of antennas is chosen at both the transmit and receive sides. Derived simple, yet tight, bounds on the performance of such systems.

(b) Hybrid Selection/Maximal-ratio Combining (H-S/MRC) Diversity Systems: Developed an analytical framework to study the performance of H-S/MRC in a multipath-fading environment. In H-S/MRC, the best L out of N diversity branches are selected and combined using MRC, yielding improved performance over L branch MRC.

(c) Efficient Evaluation of Error Rate for Hybrid Diversity Systems: Derived simple explicit bounds for assessing the error rate of hybrid diversity systems. The bounds are tight and valid for all values of signal-to-noise ratios; thus alleviating the need for complicated analysis and multiple numerical integrals. Contrary to a previous conjecture, the penalty of a hybrid diversity system relative to MRC diversity was shown not to be a constant; it is not independent of the SNR and the target symbol error probability.

(d) Reduced-Complexity Rake Receivers: Quantified the effects of spreading bandwidth on spread spectrum systems in dense multipath environments in terms of performance, complexity, and channel parameters. Developed an analytical framework that provides fundamental insights on how wideband reduced-complexity Rake receivers can best take advantage of multipath, and theoretical basis for deciding how many fingers should be included in the receiver architecture.

(e) Subset Diversity with Practical Channel Estimation: Developed an analytical framework for evaluating the performance of subset diversity schemes in the presence of channel estimation error. Showed that such a system preserves the full diversity order. The study revealed that the
asymptotic performance loss due to estimation error has a surprising lack of dependence on the number of combined branches or the total number of available diversity branches.

**Ultra-Wide Bandwidth (UWB) Communications**

Performed pioneering work on UWB radio and provided a foundation for the design of UWB wireless networks. Specific contributions include:

1. **Propagation Measurement and Statistical Modeling:** Conducted the first UWB signal propagation experiments, devised a statistical propagation channel model, and demonstrated the robustness of a UWB signal in a multipath environment.

2. **Receiver Design, Analysis and Simulations:** Proposed theoretical analysis and experimental techniques, all of which enabled the efficient design and accurate performance prediction of UWB transmission.

3. **Transmitted-Reference (TR) Signaling for UWB Communications:** Developed an analytical framework, based on a sampling expansion approach, to evaluate the performance of TR and differential TR signaling for UWB systems with autocorrelation receivers.

4. **Unified Spectral Analysis:** Derived general expressions for the PSD of a variety of time-hopping spread-spectrum signaling schemes in the presence of timing jitter using stochastic theory.

**PROF. GREGORY W. WORNELL**

Professor of Electrical Engineering

http://www.rle.mit.edu/rleonline/People/GregoryW.Wornell.html
http://www.rle.mit.edu/sia/
http://www.rle.mit.edu/cwn/
http://csbi.mit.edu/website/members/Members/gwornell

Professor Wornell's research interests span several areas of signal processing, communication networks, and information theory, and include algorithms and architectures for wireless networks, broadband systems, and multimedia environments. This research investigates a broad spectrum of issues, from fundamental limits, to algorithm structures, to implementation issues.

He leads the group's digital communication networks laboratory, which includes a wireless testbed operating in the 900 MHz range to carry out experiments on novel algorithms and architectures for wireless communications. The testbed consists of analog front-end and DSP hardware, controlled by a back-end network. Currently under development, in collaboration with Professors Sodini, Lee, and Chandrakasan of the Microsystems Technology Lab (MTL), is the architecture and systems level design for a Gigabit/sec wireless local-area network (LAN) operating in the 5.8 GHz band.

**Circuits and Algorithms for Pipelined ADCs in Scaled CMOS Technology**

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 nonlinearities 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.

**Digital Processing in Imaging Systems**

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 programatically 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.

**Secret Key Generation Using Sources and Channels**

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, satellite broadcast, channel reciprocity. The goal is to exploit these resources in conjunction with the underlying channel to develop novel techniques for key distillation.

**Secure Broadcasting Over Fading Channels**

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.

**Technologies for Streaming Media Delivery**

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.

**The Impact of Asynchronism on Communication**

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.

**Multimedia Compression with Encoder Side Information**

In many applications, there is a need for digital representations of various kinds of content. Such content includes, for example, video, audio, imagery, as well as various kinds of sensor data. To develop compact representations, one needs to take into account the semantics of the content. In particular, the goal is not to enable an exact reconstruction of the content, but rather one that is semantically indistinguishable from original for the applications of interest. In Shannon's formulation of the problem, the semantics are captured through a distortion measure. When such semantic information is shared between encoder and decoder, the fundamental rate-distortion tradeoffs are well understood. This work explores the corresponding tradeoffs when such semantic information is not universally available. We show, for example, that when only the decoder has access to the full semantics, it provides no benefit and may as well be ignored. By contrast, when only the encoder has access to the full semantics, in many cases that is sufficient to do as well as if the decoder had it too. Moreover, we show that systems in which such semantic information is measured at the encoder and shared with the decoder through a side channel -- which is the basis of many perceptual coding systems, for example -- can be particularly
inefficient. As an efficient alternative, we introduce low-complexity lattice codes in which there is a fixed codebook but a variable partition to exploit encoder-only side information.

**Ultralow-Complexity Iterative Interference Cancellation**

In many communication applications, the dominant impairment is interference. This is especially true of wireless environments. There is typically self-interference due to multipath propagation. When system bandwidths are large enough, this takes the form of intersymbol interference. However, there is also interference from other users in the next work, as well as various forms of extra-network interference. The degree to which such interference can be mitigated through signal processing within the network strongly affects the overall capacity. Thus interference-cancellation algorithms are of considerable interest. However, traditional low-complexity linear interference cancellation techniques cannot exploit enough of the structure in the interference to be effective, while maximum-likelihood (ML) interference cancellation are the most effective, but have exponential complexity. We show that in fact, the performance of ML cancellation can be approached at high SNR with a complexity that is negligibly higher than the linear techniques.

In particular, we develop an efficient convergent iterative algorithm structure that alternates between generating increasingly reliable symbol decisions and increasingly reliable interference estimates. Combining such decoding structures with a precoding technique at the encoder we refer to as mode-interleaving extends their effectiveness to a particularly broad range of channels.

**Asynchronous Communication**

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. The 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 $\alpha$ represents the "synchronization threshold" and admits a simple expression depending on the channel. The scheme we propose to reliably communicate under extreme asynchronism, perhaps somewhat surprisingly, performs detection of the codeword and isolation of the message jointly rather than separately as often in practice.

**Secure Transmission with Multiple Antennas**

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 multiantenna-
wiretap channel and develop several low complexity techniques to realize these gains for practical models.

**Hewlett-Packard Wireless Invent@MIT**

The Center for Wireless Networking's flagship project is an ambitious, highly interdisciplinary effort whose charter is to re-think the way that wireless networks and mobile appliances are designed and implemented.

A key part of its mission is to uncover the fundamental limits that govern such systems, and the forces that shape their evolution. In turn, these insights are guiding the development of a broad set of novel cross-layer design techniques to improve reliability, responsiveness, security, scalability, and energy-efficiency. The resulting improvements are expected to enable important new applications involving streaming media and other high-data rate content.

A hallmark of this project is its emphasis on pursuing innovation by bringing together diverse groups and research communities that have traditionally worked more independently. Indeed, MIT and Hewlett-Packard Laboratories are using this joint effort to re-invent the model for academic-industrial collaboration, and pioneer innovative new approaches to such interaction.

**Efficient Scheduling and Quantization for MIMO Broadcasting Systems with Limited Feedback**

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 one's 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 with m antennas, and n receiving users, where n >> m. We show that the 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.

**Information Theoretic Perspectives on Synchronization**

In Information Theory, a common assumption is that “whenever the transmitter speaks the receiver listens.” In other words, in general, there is the assumption of perfect synchronization between the transmitter and the receiver, and, basic quantities, such as the channel capacity and the coding delay, are defined under this hypothesis. In practice, this assumption is rarely fulfilled; due to the spasmodic nature of the information source, the transmitter may start emitting at random moments, and the receiver needs a certain period of time to realize that the transmitter
has started to emit information. The goal of the present project is to model the notion of synchronization, incorporate it as a basic notion into Information Theory, and propose high rate and reliable coding schemes that minimize the penalty due to a lack of synchronization.

The motivation for this project is twofold. First, in practice synchronization requires a nonnegligible amount of energy to be spent in addition to the energy used for transmitting information. Hence, short and efficient synchronization procedures are needed. Second, formulating basic quantities, such as the capacity and the reliability function of a channel, taking into account the notion of synchronization may lead to new performance criteria as well as new channel coding designs.