Research Statement

Information theory by Claude Shannon has strongly influenced the design of modern communication systems. Shannon’s approach was not always accepted as the “right” theory. Information theoretic models for sources and channels are over-simplified abstractions of real systems. Capacity theorems involve random coding techniques that are clearly impractical. Nevertheless, in the decades that followed Shannon’s work, error correction codes that closely approach the ultimate capacity limits were discovered and implemented in real systems. Interestingly, modern error correction codes involve random interleavers and probabilistic decoding and are of the same spirit as Shannon’s original work.

I draw inspiration from Shannon’s approach: important engineering problems are best understood through simplified abstractions. My recent research focuses on two areas that I believe are crucial to the success of future of wireless systems: Security and Multimedia. Today’s wireless systems fall significantly short of providing satisfactory solutions to these issues.

Traditionally mobile links are the “weak-links” in security and privacy of networked systems. Powerful, low cost attacks can be engineered by eavesdropping wireless signals and exploiting protocol flaws and user mistakes. Both cellular systems and wireless LANs are vulnerable in protecting identity, privacy and security of users. Such flawed networks are not mere annoyances, but threaten our national economy and security. My research work develops new security architectures in wireless systems that go well beyond traditional paradigms in cryptography. Such solutions involve multiple-antennas, power control mechanisms, knowledge of wireless channel characteristics and other physical layer resources. A new PHY-SEC layer, which compliments existing security solutions, can significantly increase the resistance to various attacks.

Multimedia streaming over wireless links is another major challenge we face today. The emergence of smart-phones has created unprecedented demands for data that wireless networks cannot sustain. Bandwidth efficient multimedia streaming is a top priority. Surprisingly we understand little about the fundamental limits of streaming sources. My recent project [5] proposes a new class of streaming multicast codes that significantly outperform off-the-shelf error correction codes. It introduces a new dimension of low-delay into problems in information and coding theory.

Wireless Security: Physical Layer Approach

My interest in information theoretic security developed during a summer internship at Mitsubishi Electrical Research Lab (MERL). My project, secure biometrics, involved implementing a secure biometric recognition system. Using principles of distributed source coding, this system only stores a hash of the biometric. It provides privacy to biometric systems – a problem that cryptographic techniques fail to address. Is there a deeper connection between information theory and security? I decided to pursue this direction further. Fortunately, I discovered an interesting line of work information theoretic security dating back to Claude Shannon, and became fascinated with its applications to wireless systems.
My dissertation work at MIT resolves the secrecy capacity of the multi-antenna wiretap channel (MIMOME channel). Before this work very little was known on the role of multiple antennas for secrecy. The secrecy capacity was stated as an open problem. Good lower bounds were also not known - optimizing a natural rate expression even for the restricted class of Gaussian input distributions appeared to be an intractable non-convex optimization. It therefore came as a surprise when we [1] established the secrecy capacity, demonstrated optimality of a Gaussian distribution and provided a computable expression for the capacity. Our solution did not rely on the brute-force optimization considered earlier. Instead it followed an indirect path and was inspired by a user-cooperation argument used in the MIMO broadcast channel. The time was perhaps just right for our work. Another group from Caltech reported a similar result just after our work appeared. Several follow-up papers have appeared subsequently.

Another related challenge, I recently tackled [2] was the capacity of multi-antenna compound wiretap channel. The compound extension models channel uncertainties in the MIMOME model. Its solution remains open till date. In [2], I report new progress on this problem. This work establishes a significantly tighter upper bound than a natural “pairwise upper bound” [7]. It also reports new progress on lower bounds using ideas from interference alignment and multilevel coding. These are significantly improvements over previously known rates based on Gaussian codebooks [7].

More broadly information theoretic techniques based on source and channel coding provide a new set of techniques for addressing various challenges related to security and privacy. In [3, 4] we establish fundamental limits on secret-key generation and discuss applications to sensor networks and wireless channels; in [6] we apply these ideas to smart-grid systems; whereas in [8] we study secure network coding using this framework.

**Low Delay Streaming Codes**

My interest in multimedia streaming systems developed while working on a mobile peer-to-peer video streaming application at T-Labs. I started exploring simpler abstractions to understand these systems. I soon realized that information theory provides limited insights into streaming systems. While a large body of literature on joint source-channel coding problems exists, these models are primarily suitable for image transmission — not streaming video. Practical video codecs use GOP structures to strike balance between compression efficiency, error propagation and end-to-end delay. Can information theory provide insights into such tradeoffs?

My recent work focuses on characterizing information theoretic tradeoffs for transmitting streaming sources over packet erasure channels. Several surprising results have emerged. For example, in [5] we study the problem of multicasting an i.i.d. streaming source to two receivers over an erasure broadcast channel. The receivers differ not only by the channel quality but also by their end-to-end delay. We establish the multicast capacity and obtain several interesting connections between delay and capacity. A receiver with a relatively weaker channel but a tolerating a larger delay could be “better” than a receiver with a stronger channel but a stringent delay requirement. Furthermore critical thresholds exist beyond which excess delay cannot increase the multicast capacity. More generally low-delay constraints introduce a new dimension to problems in information and coding theory that has received very little attention.
Future Work
In the near future, I expect to continue my investigations in the two areas described above: Security and Multimedia for wireless systems.

Recently, a growing body of literature in the antennas community investigates the design of “privacy beams” using reconfigurable antenna arrays. This work has the same ultimate goal as the MIMOME channel – data confidentiality using multiple antennas. It is only natural to investigate the common elements between these lines of works. New problems in information theory motivated by reconfigurable antenna arrays are likely to result from these investigations. Furthermore, applications of information theoretic security to areas such as body sensor networks, wireless health care, smart metered systems, biometrics and multimedia authentication are also fascinating topics for future research.

In the near future, I seek to develop a theory for transmission of streaming sources over wireless links. Such a theory will characterize fundamental limits on compression efficiency, error propagation across frames, end-to-end delay and distortion. It would suggest a new class of streaming error-correction codes, develop insights into new “delay-limited regimes” and more broadly examine whether current architectural solutions in video codecs are indeed efficient engineering solutions.

I select research problems inspired by current technological challenges in the communications industry. I expect my research activity in security and multimedia systems to be in line with various funding agencies. In addition, I also find interactions with researchers in industry particularly stimulating. I have developed ties with companies such as T-Labs (Palo Alto), HP Labs (Palo Alto), and Ultra-Electronics TCS (Montreal) that will certainly shape some of my research activity in the coming years. Shannon’s “right” way of looking at important engineering problems still remains my guiding principle for research.

References
3. A. Khisti " Secret-key agreement over wiretap channels with transmitter side information, European Wireless Conference, 2010
5. A. Badr, A. Khisti and E. Martinian, "Diversity Embedded Streaming Erasure Codes (DE-SCo): Constructions and Optimality" Submitted to JSAC Special Issue on Trading Rate for Delay at the transport and application layers. Conference Version: To Appear, Globecom 2010