IEEE Hamilton Section

Joint Chapter of Communications, Information Theory, and Signal Processing Societies
McMaster ECE Distinguished Speaker Series

Seminar: Thursday 2015-Nov-19 2:00 PM
Room ITB A113, McMaster University

Media-based Modulation: Surpassing Known Limits in Spectral Efficiency and Security

Amir K. Khandani
E&CE Department, University of Waterloo

The idea of Media-based Modulation (MBM) is based on embedding information in the variations of the transmission media (channel state). This is in contrast to legacy wireless systems where data is embedded in a Radio Frequency (RF) source prior to the transmit antenna. MBM offers several advantages vs. legacy systems, including "additivity of information over multiple receive antennas", and "inherent diversity over a static fading channel". MBM is particularly suitable for transmitting high data rates using a single transmit and multiple receive antennas (Single Input-Multiple Output Media-Based Modulation, or SIMO-MBM). It is shown that a 1xK SIMO-MBM over a static multi-path channel asymptotically achieves the capacity of K parallel Additive White Gaussian Noise (AWGN) channels, where for one unit of energy sent over the single transmit antenna, the effective energy for each of the K AWGN channels is one.

Complexity issues limit the amount of data that can be embedded in the channel state using a single transmit unit in SIMO-MBM. To address this shortcoming, this presentation also introduces the idea of Layered Multiple Input-Multiple Output Media-Based Modulation (LMIMO-MBM). LMIMO-MBM enables forming a high-rate constellation as superposition of constituent vectors due to separate transmit units. Relying on such a layered structure, LMIMO-MBM can significantly reduce hardware and algorithmic complexities, as well as the training overhead, vs. SIMO-MBM. Exploiting the layered constellation structure, a fast iterative algorithm is proposed for signal detection. Simulation results show excellent performance in terms of Symbol Error Rate (SER) vs. Signal-to-Noise Ratio (SNR). For example, a 4X16 LMIMO-MBM is capable of transmitting 32 bits of information per (complex) channel-use, with SER~10^{-5} at Eb/N0~-3.5dB (or SER~10^{-4} at Eb/N0~-4.5dB). This performance is achieved using a single transmission (no extension in time/frequency), and without adding any redundancy for Forward-Error-Correction (FEC). This means, in addition to its excellent SER vs. energy/rate performance, MBM relaxes the need for complex FEC structures used in legacy wireless systems, and thereby minimizes the transmission delay. Application of FEC can further improve the performance. For example, applying Reed-Solomon codes enables transmitting 30 bits of information per (complex) channel-use with a Frame Error Rate (FER)~10^{-5} at Eb/N0~-6dB. It is shown that, under a set of mild conditions, by applying FEC with error correction capability *t*, the slope of the error rate vs. SNR (with hard decision decoding) will asymptotically increase by a factor of *t+1*.

A practical (small size and low complexity) RF configuration is presented for embedding information in the channel state. For this purpose, periodic RF constructions are introduced which can act as on-off RF mirrors. The on-off operation relies on simple RF switches, for example using PIN diodes, and can support very fast switching for high bandwidth applications. It is also shown that a proper RF implementation allows implementing a NxK MIMO-MBM using a single transmit chain (instead of N).

It is shown that the same antenna configuration can be used to provide unconditional security in wireless. This is based on using a wireless channel to establish a secret key (one-time pad) between two legitimate parties. Wireless channel enables providing a reference of phase between the two legitimate parties, which in turn is used to extract a common phase value. Each such phase value can completely mask a phase-shift-keying (PSK) symbol (zero information leakage). The shared phase depends on the propagation environment between legitimate parties and will be impossible to guess even by an eavesdropper who is in close vicinity, has unlimited processing power and enjoys high signal-to-noise ratio. It is shown that the same antenna configuration used for media-based modulation can perturb the wireless channel such that a number of such common phase values can be generated, together providing a longer secure key.

BIO: Amir K. Khandani is a professor in Electrical and Computer Engineering Department of the University of Waterloo. He holds a Tier I CRC on Information Theory for Wireless Networks, and an NSERC-Ciena IRC on Information Theory for Backbone Networks. Previously, he held a Tier I CRC, the NSERC-Nortel IRC, and subsequently, the NSERC-Blackberry IRC, all on Wireless Transmission. Dr. Khandani received his degrees from Tehran University, Iran, and McGill University, Canada, in 1984 and 1992, respectively. He joined uWaterloo in 1993. Since 1993, he has supervised close to 100 graduate students, and contributed to the publication of more than 200 referred publications. Khandani's team is responsible for introducing the concept of Interference Alignment, an area widely pursued and considered a theoretical breakthrough. His team established the theory and implemented a functional prototype of the first Full-duplex Wireless node, an area that had challenged researchers for several decades.