

LDPC Codes for the Gaussian Wiretap Channel

Demijan Klinc and Steven W. McLaughlin

Georgia Institute of Technology

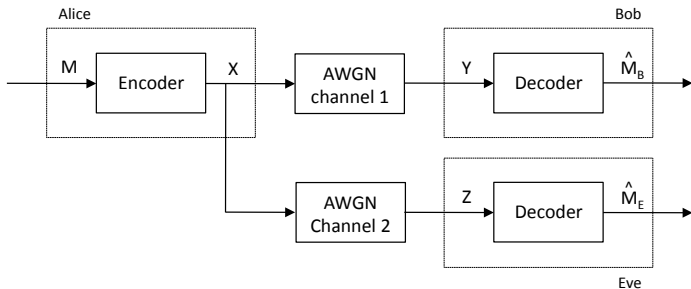
School of Information Theory @ Northwestern University

August 13, 2009

Motivation

- results from information theory tell us that security can be addressed at the physical layer
- wireless systems do not take advantage of the stochastic nature of communication channels for security; security is addressed at higher layers of the protocol stack
- we are interested in practical code constructions that operate on the physical layer and provide
 - high reliability between legitimate parties
 - no information leakage to eavesdroppers
- BER over message bits is chosen as the metric for secrecy

Gaussian Wiretap Channel



- Captures the relationship between a legitimate receiver and an eavesdropper
- Assumption: Eve is passive and her SNR is lower than Bob's

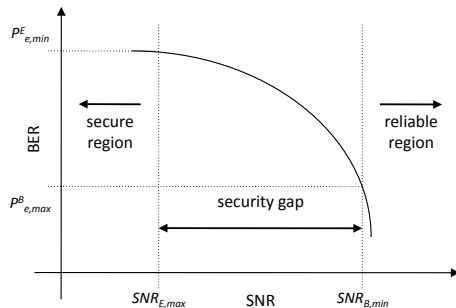
Code Design for Gaussian Wiretap Channel

- Let P_e^B be Bob's BER and let ϵ be a constant arbitrarily close to 0
- Let P_e^E be Eve's BER and let $P_{e,\min}^E$ be a predefined constant close to 0.5

Constraints:

- $P_e^B \leq \epsilon$
- $P_e^E \geq P_{e,\max}^E$

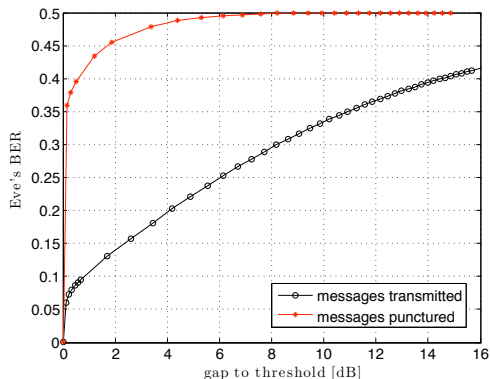
Minimize the Security Gap



Secure LDPC codes

- main idea: transmit messages over punctured bits to hide data from the eavesdroppers
- the proposed method is evaluated asymptotically using density evolution
- equivalent to bitwise-MAP decoding
- naturally extendable to finite-block length constructions

Secure LDPC Codes



- if messages are punctured, Eve's SNR grows very fast to 0.5 as her SNR deteriorates
- if Eve's signal is only a few dB lower than Bob's she is forced to BERs close to 0.5, even if she has the capability to use a bitwise-MAP decoder

Optimize Puncturing Distributions

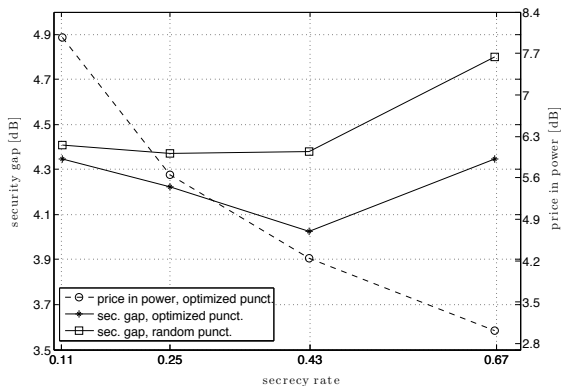
- a puncturing distribution is captured by a polynomial

$$\pi(x) = \sum_{i=2}^{d_v} \pi_i x^{i-1}$$

- the security gap of an LDPC code can be optimized by choosing an appropriate puncturing distribution
- the optimization is generally non-linear and we used differential evolution to obtain optimized puncturing distributions with small security gaps, by solving

$$\arg \min_{\pi_i \text{'s}} (\text{security gap})$$

Performance of Optimized Secure LDPC Codes



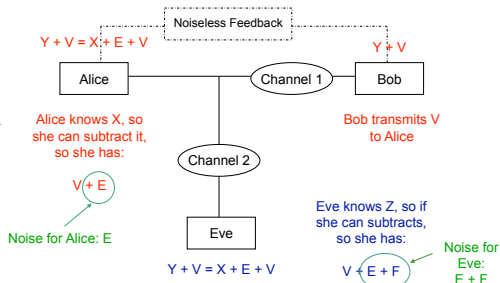
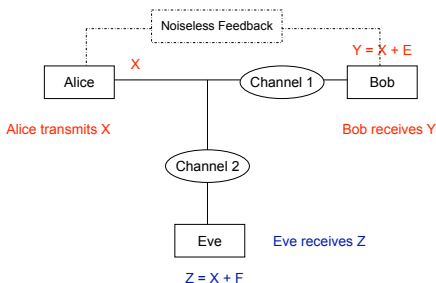
- puncturing pattern is optimized for security
- the codes are efficiently encodable
- problem: increased transmission power

Addressing Power Loss

- in essence, the reason our codes exhibit small security gaps is because they are non-systematic
- power loss could possibly be diminished by using a different type of non-systematic LDPC codes, i.e. with scrambled information bits
- challenge: develop theoretical framework to show their security potential (as we did for punctured LDPC codes)
- **ultimate goal: secure error-correction codes that have small security gaps and do not incur power losses**

What if Eve's SNR is better than Bob's ?

- previously assumed: Eve's SNR is worse than Bob's
- if Eve's SNR is better than Bob's, feedback can help (example from [Maurer, 93])



Practical code constructions with feedback

- we want to study practical code constructions that will rely on feedback to enable secure communications when Eve has a better SNR than Bob
- consider scenarios with noiseless and noisy feedback
- consider scenarios with multiple legitimate receivers/multiple eavesdroppers

Summary

- we propose a practical code construction based on LDPC codes for physical layer security
- BER grows very fast to 0.5 even if an eavesdropper has the ability to use a bitwise-MAP decoder
- codes are efficiently encodable and the construction can be extended to finite-block lengths for practical applications
- issue: increased transmit power