Physical Communication 24 (2017) 94–102

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Performance of lattice coset codes on Universal Software Radio Peripherals

Jinlong Lu, J. Harshan *, Frédérique Oggier

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

ARTICLE INFO

Article history:
Received 5 January 2017
Received in revised form
9 April 2017
Accepted 18 April 2017
Available online 2 May 2017

Keywords:
Physical-layer security
Coset coding
Eavesdropping
Lattice codes
USRP

ABSTRACT

We consider an experimental setup of three Universal Software Radio Peripherals (USRPs) that implement a wiretap channel, two USRPs are the legitimate players Alice and Bob, while the third USRP is the eavesdropper, whose position we vary to evaluate information leakage. The experimented channels are close to slow fading channels, and coset coding of lattice constellations is used for transmission, allowing to introduce controlled randomness at the transmitter. Simulation and measurement results show to which extent coset coding can provide confidentiality, as a function of Eve's position, and the amount of randomness used.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

We consider a wiretap channel, comprising a legitimate transmitter, Alice, and two receivers: a legitimate one, Bob, and a passive adversary, Eve. For the legitimate users Alice and Bob, both reliable and confidential transmission needs to be achieved, while Eve is trying to eavesdrop the communication. This is done through wiretap coding. Alice encodes her secret $\mathbf{s}$ into a codeword $\mathbf{x}$ belonging to a code $\mathcal{C}$, and $\mathbf{x}$ is then sent through the wiretap channel to Bob and Eve, which respectively receives $\mathbf{y}_B$ and $\mathbf{y}_E$. What distinguishes wiretap coding from standard coding is the constraint on confidentiality, which should be obtained without invoking cryptographic means: confidentiality is obtained by a suitable injection of controlled randomness mixed with an appropriate coding strategy at the transmitter, which enables Bob to receive his message with high probability, while confusing the eavesdropper to the point of making her knowledge of the secret message negligible. This is formally expressed by saying that the mutual information between what Eve receives and the secret is zero:

$$I(\mathbf{s}; \mathbf{y}_E) = H(\mathbf{s}) - H(\mathbf{s}|\mathbf{y}_E) = 0 \tag{1}$$

or equivalently, that the entropy $H(\mathbf{s}|\mathbf{y}_E)$ of the secret knowing the received message at the eavesdropper is the same as the entropy of the secret.

Wiretap coding necessarily requires the channel from Alice to Bob to be different from that from Alice to Eve. What "different" means, as well as wiretap coding strategies, depend on the channel model, e.g., discrete memoryless, additive white Gaussian, Rayleigh fading, or multiple-input multiple-output (MIMO), to name a few popular models. We refer the readers to [1,2] for a survey of information theoretic results and respective coding strategies for wiretap channels, and to [3–5] for application of practical codes on wiretap channels.

In all cases, the channel assumptions, in particular regarding the eavesdropper's channel, are critical, since the confidentiality analysis relies on them. This is the case for wiretap coding, but also for any other schemes whose security relies on channel noise, such as secret key generation.

The goal of this paper is to study wiretap coding from an experimental view point using a USRP testbed comprising three USRPs, one for each of the three players, Alice, Bob and Eve. The channels between Alice and Bob, and Alice and Eve respectively, are close to slow fading channels, whose SNRs and noise are given by the experimental settings. Transmission is done using signal constellations from lattices, which are transmitted using coset coding as explained in Section 2, to introduce controlled randomness (for that reason, we will use the term "coset coding" rather than wiretap coding in the rest of the paper). The positions of Alice and Bob are kept fixed, while we vary the position of Eve to analyze her received signal, and how much information is leaked depending on both her position and the coding scheme used.

We present both simulations and experimental results that consistently show how coset coding does provide confusion at the

* Corresponding author.
E-mail addresses: kerin_lu@ntu.edu.sg (J. Lu), jharshan@ntu.edu.sg (J. Harshan), frederique@ntu.edu.sg (F. Oggier).

http://dx.doi.org/10.1016/j.phycom.2017.04.004
1874-4907/© 2017 Elsevier B.V. All rights reserved.

eavesdropper, with entropy (see Section 2.2) and decoding error as metrics, using an optimal decoder for Eve, as proven in Section 2.3. Extensive results are provided in Section 3 and Section 4, to compare coset coding versus conventional coding, but also different coding schemes using lattice constellation of different dimensions, different amounts of randomness and different positions for Eve. Experiments were realized by transmitting "the cameraman image" (see Fig. 4), which furthermore allows a visualization of the effect of coset coding (see Fig. 12).

We believe that this type of experimental work is critical to the development of physical layer security, since it gives an insight of how practical a security scheme such as coset coding behaves in practice, without having to rely on channel assumptions. To the best of our knowledge, this is the first work that demonstrates the application of wiretap lattice codes on a software defined radio testbed. Another work with the same philosophy was done for key generation in [6], where the authors investigate the role of the eavesdropper's statistics when actually implementing a secret-key generation system over a wireless channel. This is done via a software-defined radio testbed, where the channel gains are measured. The experimental setup shows a 20% loss in secret-key rate with respect to theoretical bounds.

2. Coset encoding of lattice codes

We consider a wiretap testbed formed by three USRPs, as shown on Fig. 1. One USRP plays the role of the legitimate transmitter Alice, while the other two USRPs are the receivers, Bob and Eve.

This wiretap channel is modeled by

$$\mathbf{y}_B = h_B\mathbf{x} + \mathbf{n}_B \tag{2}$$

$$\mathbf{y}_E = h_E\mathbf{x} + \mathbf{n}_E \tag{3}$$

where $h_B, h_E \in \mathbb{C}$ are the respective channel gains, $\mathbf{x} \in \mathbb{C}^{L/2}$ is the transmitted message (L is the real dimension, an even number), and $\mathbf{n}_B, \mathbf{n}_E$ are the respective channel noises at Bob and Eve, distributed as circularly symmetric complex Gaussian, denoted by as $\mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}_{L/2})$.

To transmit over this complex channel, we consider lattice coding. A real lattice Λ of dimension L is a discrete set of points in $\mathbb{R}^L$ generated as integral linear combinations of a set of L linearly independent vectors in $\mathbb{R}^L$. For actual data transmission, a finite constellation of the lattice is chosen. For example, constellations from Quadrature Amplitude Modulation (QAM) are obtained by taking a finite subset of the lattice $\mathbb{Z}^L$. When L is even, a real lattice can be used for transmission over a complex channel of dimension $L/2$. The role of a lattice encoder is to map a bit string to a lattice point. However for wiretap coding, we use instead lattice coset coding, which allows us to introduce randomness.

2.1. Lattice coset coding

At the transmitter, we implement a lattice coset encoder. A lattice coset encoder requires two nested lattices $\Lambda_E \subset \Lambda_B$, and a partition of Λ_B as a union of cosets of Λ_E:

$$\Lambda_B = \bigcup_{\mathbf{s}\in\Lambda_B/\Lambda_E} (\mathbf{s} + \Lambda_E) \tag{4}$$

where $\mathbf{s}$ is a coset representative. In Fig. 2, a lattice Λ_B is shown as the union of the lattice $\Lambda_E = 2\mathbb{Z}^2$ and its coset $2\mathbb{Z}^2 + (1, 1)$.

In the context of wiretap coding, coset coding is used to create confusion by introducing controlled randomness. In this case, $\mathbf{s}$ actually encodes the secret, while a vector $\mathbf{r}$ is chosen randomly inside Λ_E, to obtain $\mathbf{x} = \mathbf{s} + \mathbf{r}$. We use the index B in Λ_B to indicate that this lattice is used for transmission to Bob, while Λ_E is the lattice meant to create confusion at Eve's end.

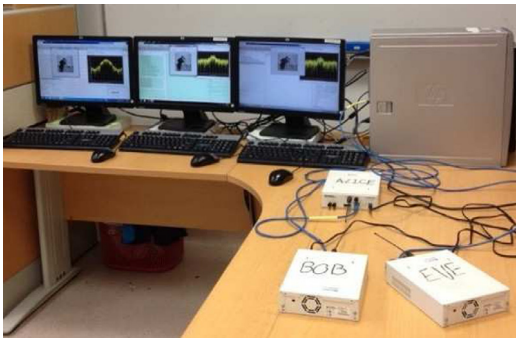

Fig. 1. USRP testbed, comprising three USRPs: a transmitter (Alice) and two receivers (Bob and Eve).

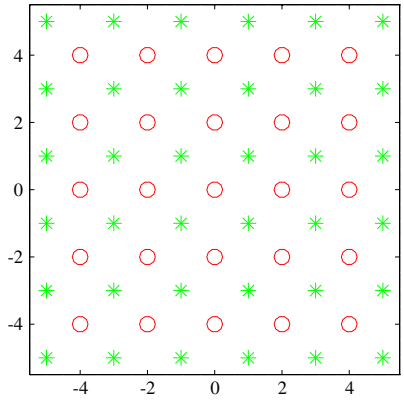

Fig. 2. The lattice D_2 obtained via Construction A. The circles are used for the lattice $2\mathbb{Z}^2$, and the stars for the coset $2\mathbb{Z}^2 + (1, 1)$.

Table 1
Lattices via Construction A: $\Lambda = 2\mathbb{Z}^L + C$.

Λ	L	C
$\mathbb{Z}^2$	2	{00, 01, 10, 11}
D_2	2	{00, 11}
D_4	4	(4, 3, 2) parity check
$\sqrt{2}E_8$	8	(8, 4, 4) Reed–Müller

A partition of Λ_B as a union of cosets of a sublattice Λ_E can be obtained using the so-called Construction A [7]. Let $\rho : \mathbb{Z}^L \to \{0, 1\}^L$ denote the componentwise reduction modulo 2, which maps an integral vector to a binary one. In $\{0, 1\}^L$, choose a binary linear code C of length L and dimension k. Then we take for Λ_B the lattice $\rho^{-1}(C) = 2\mathbb{Z}^L + C$ (possibly scaled), and thus $\Lambda_E = 2\mathbb{Z}^L$. Codewords from C are the coset representatives. The lattice on Fig. 2 is called D_2, and is actually obtained using Construction A and the repetition code $C = \{(0, 0), (1, 1)\}$:

$$D_2 = 2\mathbb{Z}^2 + C = (2\mathbb{Z}^2 + (0, 0)) \cup (2\mathbb{Z}^2 + (1, 1)).$$

Table 1 lists different Construction A of lattices that we use.

For an infinite lattice, the vector $\mathbf{r}$ introduced for randomness is chosen according to the uniform distribution. To perform experiments, finite constellations are carved from lattices, by taking lattice points in the hypercube $\{0, 1, 2, \ldots, M - 1\}^L$, and we keep the choice of a uniform distribution for the randomness used (a possibility for further experiments could be to use instead the distribution proposed in [8]).

In what follows, we use the terminology *standard* or *conventional encoding* to refer to lattice coding (say data points are mapped to points in D_2 or E_8) without use of randomness, in contrast to *coset encoding* which introduces randomness as explained above.

Download English Version:

https://daneshyari.com/en/article/4957604

Download Persian Version:

https://daneshyari.com/article/4957604

Daneshyari.com