Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 319–323*

Towards to Anonymity in Physical-Layer Network Coding [1]

Oksana Trushina oksana.trushina@gmail.com
Moscow Institute of Physics and Technology

Abstract. In this paper we consider two successive Gaussian wiretap channels from a source to a relay and from the relay to a receiver. Gaussian channel is a common model of wireless network. There is an adversary who can eavesdrop both channels and analyse obtained signals. The task is to organize data transmission from the source to the receiver so that the signals obtained by adversary are unlinkable from his point of view. We base on the existence of secure lattice coset codes and use coset coding strategy. Our approach is to choose random point from Voronoi cell of incoming lattice point at the relay side and transmit further this random point. Owing to secure lattice code the receiver can decode signal correctly while the adversary cannot get any information. We believe our approach may be applied to physical layer network coding.

1 Introduction

Network coding is a conception of data transmission where relay network nodes may perform operations with input packets. For example, they can form linear combinations of input packets and transmit further that combinations. In wireless networks such operations may be performed naturally on physical layer thanks to electromagnetic waves superposition – the electromagnetic waves encountering in the same point of space add together. A use of nested lattice codes in physical layer network coding realizes a compute-and-forward relaying strategy [1] which is being widely studied. The strategy seems to be practical because there is no need of channel state information at the transmitters.

In this paper we consider an approach to anonymous transmission which can be applied to nested lattice based physical network coding. The transmission of a message is anonymous if it is impossible for an adversary to trace the message, in other words the adversary cannot determine who communicates with whom. A passive adversary who can only eavesdrop messages and analyses them is considered. Our approach is based on lattice coset encoding strategy for Gaussian wiretap channel. The present work is motivated by recent results described in [2] and [3]. The papers propose code design criteria and prove that

[1] This research is partially supported by the Russian Foundation for Basic Research, project № 12-07-00122-a.

nested lattice code can provide secrecy over Gaussian wiretap channel. Relying on that we place one relay node between source and destination and describe approach according which the relay node can recompute incoming signals for further transmission so that the adversary cannot relate incoming and outgoing signals of the relay node.

2 Preliminaries

In this section we briefly recall some basic concepts about lattices.

A real n-dimensional lattice Λ is a set of points over $\mathbb{R}^n$. It can be specified by a set of m linear independent vectors forming generator matrix G. The lattice consists of all $\mathbb{Z}$-linear combinations of generator matrix vectors

$$\Lambda = \{vG \mid v \in \mathbb{Z}^m\}.$$

A theta series of given lattice $\Lambda \subset \mathbb{R}^n$ is defined as

$$\Theta_\Lambda(z) = \sum_{x \in \Lambda} q^{\|x\|^2}, q = e^{i\pi z},\ \mathrm{Im}(z) > 0.$$

The Voronoi cell $V_\Lambda(p)$ associated with each point p of the lattice is defined as a set of points that are closest to p

$$V_\Lambda(p) = \{x \in \mathbb{R}^n \mid \|x - p\| \leq \|x - p'\|\ \forall p' \in \Lambda\}.$$

Clearly, $V_\Lambda(p) = V_\Lambda(0) + p$.

3 Secure Wiretap Lattice Codes

In this section we briefly describe coset encoding concept and results presented in [2], [3] what we base on.

Gaussian wiretap channel represents a broadcast channel where the source communicates with receiver while adversary can eavesdrop the transmission (Fig. 1). The lattice code is used so the source messages $s \in S = \{0,1\}^l$ are mapped to $x \in \Lambda$. Then the signals at the receiver and adversary correspondingly are

$$y = x + u_r,$$
$$z = x + u_a,$$

where u_r denotes a noise at the receiver and u_a is a noise at the adversary. Either of the noises is the Gaussian noise with zero mean and variance σ_r^2 for receiver channel and σ_a^2 for adversary channel.

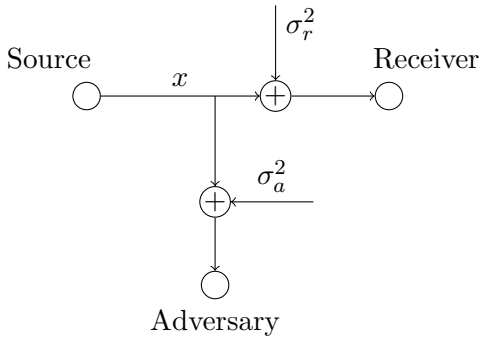

Figure 1: Gaussian wiretap channel

The messages to be transmitted securely coset coding is used. The coset coding strategy allows to confuse adversary by adding randomness. The source message is mapped not to particular codeword but instead to a set of codewords, namely a coset. Then a random point of the coset is transmitted. Thus some sublattice needs to be chosen and the whole lattice is partitioned with the sublattice. Denote the whole lattice as Λ_r because it is chosen to provide the receiver with reliability in terms of low error probability. While the sublattice is denoted as Λ_a because it is needed to adversary confusion. So the lattice Λ_r can be represented as

$$\Lambda_r = \cup_{i=1}^{2^k}(\Lambda_a + c_i),$$

where $c_i \in \mathbb{R}^n$. In this case there are 2^k cosets, hence k bits of transmitted point define chosen coset and consequently carry the information, while the remain bits carry the randomness.

Two different approach to wiretap lattice code design are presented in [2], [3]. The information theory approach is proposed in [3]. The mutual information between random variables $\mathcal{S}$ and $\mathcal{Z}$ represent source message and message received by adversary $I(\mathcal{S}, \mathcal{Z})$ is upper bounded with the bound depending on theta series of sublattice Λ_a at the point $\frac{1}{2\pi\sigma_a^2}$. So for secure transmission the theta series $\Theta_{\Lambda_a}(\frac{1}{2\pi\sigma_a^2})$ should be minimized. The existence of good wiretap codes was proved. The same results was leaded by adversary correct decision probability analysis presented in [2]. This probability is also upper bounded. The bound is also depend on $\Theta_{\Lambda_a}(\frac{1}{2\pi\sigma_a^2})$. To design good wiretap code is equivalent to find lattice Λ_r which provides receiver with correct decoding probability close to 1, and which contains a sublattice Λ_a that minimizes $\Theta_{\Lambda_a}(\frac{1}{2\pi\sigma_a^2})$. The explicit code examples were given.

4 Providing Anonymity

Based on existence of good wiretap lattice codes and inspired by progress in wiretap lattice code design we propose an approach of anonymous transmission based on coset coding.

A relay node is placed between the source and the receiver. The channels between the source and the relay and between the relay and the receiver are

both Gaussian channels with zero mean and variances $\sigma^2_{r_1}$ and $\sigma^2_{r_2}$ respectively. We consider adversary who can eavesdrop both channels. The noise at the adversary side is the Gaussian noise with zero mean and the same variance σ^2_a in both cases (Fig. 2).

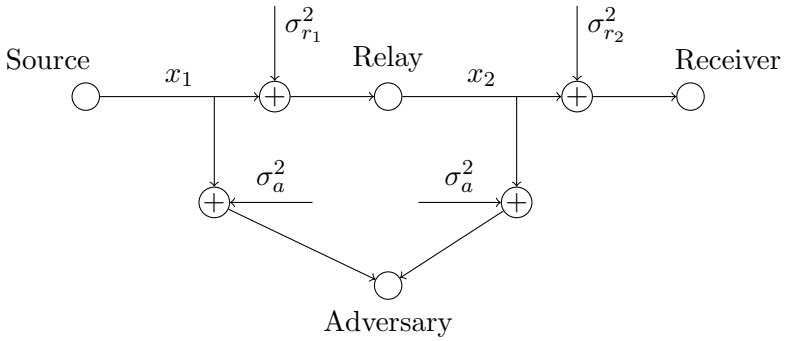

Figure 2: Model of transmission

It is worth mentioning that the task of anonymity transmission is nonsensical in above model because there are only one source and only one receiver. But to describe our approach without overflowing the explanation with details this toy model is enough.

The aim is to change incoming signal at the relay side so that the adversary cannot relate outgoing and incoming signals of the relay. The information is carried by chosen coset and so the coset cannot be changed at relay side.

The secure coset code is used. So two lattices Λ_r and Λ_a, $\Lambda_a \subset \Lambda_r$ are defined. The lattice Λ_r guarantees reliable communication between the source and the relay and between the relay and the receiver. The relay can correctly decode a signal from the source and the receiver can in turn correctly decode a signal from the relay. The lattice Λ_a ensures the adversary correct decision probability for signal eavesdropped either on the source or on the relay to be negligible.

The signal received by the relay is

$$y_1 = x_1 + u_{r_1},$$

where point x_1 belongs to certain coset $\Lambda_a + c$. The relay operates as follows in order for the outgoing signal $y_2 = x_2 + u_{r_2}$ to carry information about the same coset. First, it decodes incoming signal y_1 obtaining x_1. Then it chooses random point x_2 from $V_{\Lambda_r}(x_1)$. The relay may compute only $V_{\Lambda_r}(0)$ and get Voronoi cell for any lattice point via shifting. Finally, it transmits x_2 to the receiver. Note that the point x_2 is not a lattice point. But the receiver may decode y_2 successfully since y_2 is in $V_{\Lambda_r}(x_1)$ with high probability due to appropriate choosing of Λ_r.

The adversary has

$$\begin{cases} z_1 = x_1 + u_{a_1}, \\ z_2 = x_2 + u_{a_2}. \end{cases}$$

The z_1 and z_2 are not correlated because change in z_1 doesn't lead to change in z_2 in regular manner. To our knowledge the adversary has limited set of analysis ways. He can decode z_1 and z_2 obtaining x_1 and x_2 and analyse if one of them belongs to Voronoi cell of the other. But probability of this is low because of secure lattice code. To analyse linear combinations of z_1 and z_2 doesn't get additional information.

5 Conclusion

In this work we have addressed the problem of achieving signals unlinkability in sequence of Gaussian wiretap channels which model wireless network. The simple approach based on coset coding was described. The existence of secure lattice code was extensively used. The proposed approach is generic since it doesn't depend on specific code. We believe this approach may be applied to physical layer network coding.

Acknowledgment

The author would like to thank Prof. E. Gabidulin for helpful and fruitful discussions.

References

[1] B. Nazer, M. Gastpar, Compute-and-forward: Harnessing interference through structured codes, *IEEE Trans. Inf. Theory,* v. 57, n. 10, 6463–6486, 2011.

[2] F. Oggier, P. Solé and J.-C. Belfiore, Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis, submitted to *IEEE Transactions on Information Theory,* available on arXiv:1103.4086v3 [cs.IT], Jan 2013.

[3] C. Ling, L. Luzzi, J.-C. Belfiore and D. Stehlé, Semantically Secure Lattice Codes for the Gaussian Wiretap Channel, submitted to *IEEE Transactions on Information Theory,* available on arXiv:1210.6673v3 [cs.IT], Nov 2013.