# Amplify-and-Forward Compressed Sensing as a PHY-Layer Secrecy Solution in Wireless Sensor Networks

J.E. Barceló-Lladó, Antoni Morell, Gonzalo Seco-Granados
Dpt. Telecom. and Syst. Engineering
Universitat Autònoma de Barcelona, Bellaterra 08193 - Barcelona, Spain
{joanenric.barcelo,antoni.morell,gonzalo.seco}@uab.es

***Abstract*—Results in distributed compressed sensing show that this technique can be applied to wireless sensor networks in order to reduce the power consumption and the amount of channel uses. In this paper we extend such results with the study of the physical layer secrecy performance. In particular, we focus on an amplify-and-forward compressed sensing scheme (AF-CS) for the case when malicious eavesdropping nodes are listening. We demonstrate that this scheme achieves perfect secrecy in presence of one eavesdropper (and also for a small number of them). We also show that a very high number of eavesdropping nodes are required to perfectly recover the signal in comparison to other distributed compressed sensing schemes in the literature.**

*Keywords*– Compressed sensing, distributed schemes, physical layer secrecy, sparse signals, wireless sensor networks.

## I. Introduction

*Physical layer secrecy* provides protection against malicious eavesdroppers without the need of exchanging cryptographic keys that are used to encode the message in the higher layers. Thus the extra energy cost in terms of computing complexity and signaling is reduced. This complexity turns out to be an important drawback in a *Wireless Sensor Network* (WSN), since it is typically conformed of many small nodes that are battery and hardware limited.

*Compressed Sensing* (CS) is a signal processing tool that allows us to sample the signals below the Nyquist rate [1], and it is specially powerful in scenarios where the signals are sparse or compressible in a certain basis domain, as in image signal processing or detection. However, recent works propose CS as a secrecy technique, e.g., the authors in [2] propose a CS scheme to encrypt the measurements in addition to the already-mentioned compression properties of CS. However, the exchange of the *sensing matrix* as the key to encrypt and decrypt the message is needed, and hence this scheme does not have the benefits of *physical layer secrecy* in front of the secrecy obtained in higher layers. Furthermore, other works such as [3] propose a CS framework that establishes a secure physical layer transmission. However, the considered scenario is a point-to-point communication that involves only a single transmitter that compresses the signal, one receiver and one eavesdropper. Hence, this scenario follows a *centralized* approach that is not directly applicable to our scheme due to the *distributed* nature of the WSN environment.

Following a distributed approach, the authors of [4] propose a CS scheme applied to WSNs named *Compressed Wireless Sensing* (CWS). In such a scheme, all the sensors send synchronously only their most relevant contributions in different time slots to the fusion center.

On the other hand, we consider the *distributed* CS scheme proposed in [5] based on an *Amplify-and-Forward* (AF) scheme and named AF-CS throughout this paper. The authors have already demonstrated the ability of the AF-CS algorithm to reduce the *energy consumption* using, at the same time, a very limited number of *channel uses* and following the *distributed* approach of WSNs. In this paper we will address the secrecy level of this CS scheme in presence of a group of *coordinated and passive eavesdroppers*.

In order to provide the so-called physical layer secrecy, the system takes advantage of the linear combinations that take place *on the air* thanks to the *Multiple Access Channel* (MAC). This idea comes from the *Network Coding* theory, where the messages are not treated as indivisible, but instead, algebraic manipulations are allowed. Roughly speaking, the signal is encoded using the *channel matrix* (i.e., the *sensing matrix* in CS literature) and an eavesdropper alien to the network will not be able to decode the signal without its knowledge.

In this paper we show that we can ensure *perfect secrecy* in presence of one eavesdropper (and also in presence of a small number of them). Therefore, many eavesdroppers working cooperatively would be needed in order to recover the signal.

The contributions of this paper are as follows:

1) We extend our previous algorithm scheme in [5], analyzing it from a physical layer secrecy point of view. We find out that not only it is efficient in terms of energy and channel uses but also secure against passive eavesdropping.

The work has been supported by the Spanish Government under project TEC2011-28219, and the Catalan Government under grant 2009 SGR 298.

2) We present a design condition for the required number of eavesdropping nodes to guarantee exact reconstruction with high probability.
3) We compare our proposed AF-CS with CWS and we find out that AF-CS dramatically increases the protection agains eavesdropping at physical layer.

The rest of the paper is organized as follows: In Section II we present the system model. Section III discuses the secrecy properties of the proposed algorithm. Simulation results are given in Section IV, and conclusions are drawn in Section V.

## II. System Model

We consider a WSN configured in star-topology that monitors a given physical scalar magnitude (e.g., temperature, humidity) or detects a physical event (e.g., wildfire). In particular we assume the scheme in Figure 1, that is:

- A set $\mathcal{S}$ of $S$ *sensing nodes* connected (wirelessly) to one *fusion center*. Their measurements at discrete time $n$ are represented by $\mathbf{x}(n)$.
- A subset $\mathcal{K}(n) \subseteq \mathcal{S}$ (of cardinality $K$) of *active sensors* that are transmitting at a given time $n$. The transmitted vector is $\mathbf{x}_K(n)$ where only $K$ positions are different to zero. The remaining sensors in $\mathcal{Q}(n) = \mathcal{S} \setminus \mathcal{K}(n)$ (of cardinality Q) remain silent.
- A subset $\mathcal{R} \subseteq \mathcal{S}$ (of cardinality $R$) acts as *relay nodes* in AF mode.
- A set $\mathcal{E}$ (of cardinality $E$) of malicious and passive *eavesdropping nodes*.

Furthermore we consider the following assumptions:

A1) The *fusion center* has perfect channel information of all the links between a node in $\mathcal{K}(n)$ and a node in $\mathcal{R}$. One possibility is to estimate the channel matrix previously during a *training phase* at the network setup. On the other hand, the nodes in $\mathcal{E}$ do not have the channel information between the nodes in $\mathcal{K}(n)$ and $\mathcal{R}$. Instead, the eavesdroppers have a degraded version of the channel matrix of all the links between $\mathcal{K}(n)$ and $\mathcal{E}$.
A2) The *fusion center* knows the second order statistics of the signal of interest. The covariance matrix can also be estimated during an initial training phase. Thus the eavesdroppers do not have full access to this information.

**Notation**. Boldface upper-case letters denote matrices, boldface lower-case letters denote column vectors, and italics denote scalars. $(\cdot)^T, (\cdot)^*, (\cdot)^H$ denote transpose, complex conjugate, and Hermitian respectively. $[\mathbf{X}]_{i,j}$, $[\mathbf{x}]_i$ is the ($i$th, $j$th) element of matrix $\mathbf{X}$, and $i$th position of vector $\mathbf{x}$, respectively. $[\mathbf{X}]_i$ denotes the $i$th column of $\mathbf{X}$. Let $\mathbf{a}_K$ be a $K$-sparse approximation of $\mathbf{a}$. $|\cdot|$ is the absolute value. $\|\mathbf{a}\|_{l^1}$ and $\|\mathbf{a}\|$ mean the $l^1$-norm and the Euclidean norm of $\mathbf{a}$ respectively. Let $\hat{a}$ name the estimated value of variable $a$. $\mathbb{E}[\cdot]$ is the statistical expectation. $\mathbf{0}$ denotes the zero matrix. $(a)^+$ is the maximum between the real value $a$ and zero. Let $a \sim \mathcal{N}(\mu, \sigma_a^2)$ denote a Gaussian-distributed random variable with mean $\mu$ and variance $\sigma_a^2$.

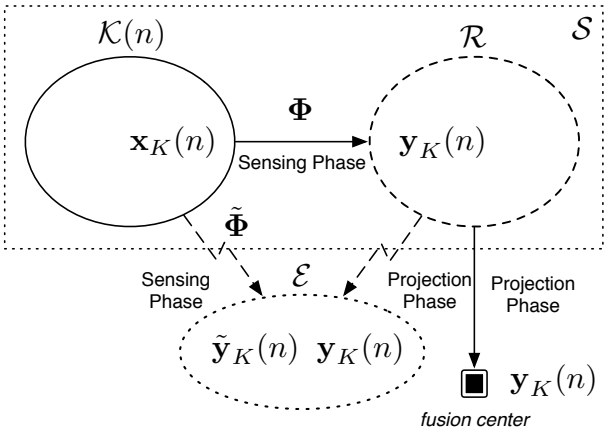


Fig. 1. MAC scenario composed by $K$ *active sensing nodes*, $R$ *relay nodes*, $E$ *eavesdropping nodes*, and one *fusion center*.

## III. Compressed Sensing Against Eavesdropping

In this paper, we consider the AF-CS algorithm developed by the authors in [5], which is summarized in the following three phases:

1) *Sensing phase*. It proposes a *distributed* method in order to select the $K$ most relevant readings of the transmitted vector $\mathbf{x}(n) \in \mathbb{R}^S$ based on the inner time correlation. These readings are collected in a $K$-sparse vector, $\mathbf{x}_K(n) \in \mathbb{R}^K$ and broadcasted time-synchronized using analog transmissions to the *relay nodes*.
2) *Projection phase*. Each relay has received linear combinations of $\mathbf{x}_K(n)$ thanks to the MAC, modeled by the *sensing matrix*, $\mathbf{\Phi} \in \mathbb{R}^{R \times S}$. Then, it relays them in AF mode to the *fusion center* using a given orthogonal transmission (e.g., frequency multiplexing).
3) *Reconstruction phase*. The *fusion center* collects the projections from all the relays in the vector $\mathbf{y}(n)$ and solves the $l^1$-norm minimization program $\mathcal{P}1$ [1],

$$\mathcal{P}1: \quad \underset{\hat{\mathbf{x}}_K(n) \in \mathbb{R}^S}{\text{minimize}} \quad \|\hat{\mathbf{x}}_K(n)\|_{l^1} \quad \text{subject to} \quad \mathbf{y}(n) = \mathbf{\Phi}\hat{\mathbf{x}}_K(n) \tag{1}$$

in order to obtain an accurate reconstruction of $\mathbf{x}_K(n)$, named $\hat{\mathbf{x}}_K(n)$. Afterwards, the *fusion center* completes the remaining $Q$ entries of the vector $\mathbf{x}(n)$ using a linear prediction in order to get the full $\hat{\mathbf{x}}(n)$.

### A. Eavesdropping in the Sensing Phase

This is perhaps the most vulnerable phase of the CS algorithm to be eavesdropped.

All the sensors in $\mathcal{K}(n)$ broadcast their readings, and hence the relay sensors receive linear combinations due to the nature of the MAC, namely,

$$\mathbf{y}(n) = \mathbf{\Phi}\mathbf{x}_K(n) + \mathbf{z}_r(n), \tag{2}$$

where $\mathbf{y}(n) \in \mathbb{R}^R$ stacks all the received signals of the nodes in $\mathcal{R}$, the sensing matrix $\mathbf{\Phi}$ models the channel between $\mathcal{K}(n)$

and $\mathcal{S}$ as a random matrix with i.i.d. gaussian entries with zero mean and variance $\sigma^2_{\mathbf{\Phi}}$. Finally, $\mathbf{z}_r(n)$ denotes white gaussian noise with zero mean and variance $\sigma^2_{\mathbf{z}}$.

Similarly to (2), the received signal at the $e$th eavesdropper is:

$$[\tilde{\mathbf{y}}(n)]_e = [\tilde{\mathbf{\Phi}}]_e \mathbf{x}_K(n) + [\mathbf{z}_e(n)]_e. \tag{3}$$

where $\tilde{\mathbf{y}}(n)$ stacks the signals received by the nodes in $\mathcal{E}$, and $\tilde{\mathbf{\Phi}}$ models the channel between $\mathcal{K}(n)$ and $\mathcal{E}$ and has the same statistics of $\mathbf{\Phi}$ and $\mathbf{z}_e(n)$ denotes white gaussian noise with zero mean and variance $\sigma^2_{\mathbf{z}}$. Then, the *coordinated* eavesdroppers would have to jointly solve the following problem:

$$\begin{aligned} \mathcal{P}2: \quad & \underset{\hat{\mathbf{x}}_K(n)\in\mathbb{R}^S}{\text{minimize}} \quad && \|\hat{\mathbf{x}}_K(n)\|_{l^1} \\ & \text{subject to} && \tilde{\mathbf{y}}(n) = (\tilde{\mathbf{\Phi}} + \mathbf{\Sigma})\hat{\mathbf{x}}_K(n). \end{aligned} \tag{4}$$

where $\mathbf{\Sigma} \in \mathbb{R}^{E\times S}$ is a random matrix with i.i.d. gaussian entries with zero mean and variance $\sigma^2_{\mathbf{\Sigma}}$ that models the errors in the channel estimation.

For *low values* of $E$ (i.e., $E < K$) the rank of $\tilde{\mathbf{\Phi}} + \mathbf{\Sigma}$ is $\text{rank}(\tilde{\mathbf{\Phi}} + \mathbf{\Sigma}) = E$ with overwhelming probability [6] and thus the reconstruction of $\mathbf{x}_K(n)$ will be a $E$-sparse signal (instead of $K$-sparse) [2]. In this case, the system experiments *perfect secrecy*. On the other hand, for *high values* of $E$ (i.e., $E > K$) one cannot assure perfect secrecy. Nevertheless, in order to ensure a *perfect reconstruction*, the matrix $\tilde{\mathbf{\Phi}}$ should hold the *Restricted Isometric Property* (RIP) condition as defined next.

*Definition 1* [7]: A matrix $\tilde{\mathbf{\Phi}} + \mathbf{\Sigma}$ satisfies the RIP of order $K$ if there exists a $\delta_K \in (0, 1)$ such that

$$(1 - \delta_K)\|\mathbf{x}\|^2 \leq \|[\tilde{\mathbf{\Phi}} + \mathbf{\Sigma}]_K \mathbf{x}\|^2 \leq (1 + \delta_K)\|\mathbf{x}\|^2, \tag{5}$$

where $[\tilde{\mathbf{\Phi}} + \mathbf{\Sigma}]_K \in \mathbb{R}^{E\times K}$ is formed by retaining any set of $K$ (or less) columns from $\tilde{\mathbf{\Phi}} + \mathbf{\Sigma}$ and $\mathbf{x}$ is any arbitrary vector of dimension $K$ (or less). For the ideal case of *perfect channel estimation* (i.e., $\mathbf{\Sigma} = \mathbf{0}$) , the condition in equation (5) is equivalent to require all the eigenvalues of $\mathbf{\Omega} = [\tilde{\mathbf{\Phi}} + \mathbf{\Sigma}]_K^T [\tilde{\mathbf{\Phi}} + \mathbf{\Sigma}]_K \in \mathbb{R}^{K\times K}$, to be inside the interval $[1-\delta_K, 1+\delta_K]$ [8]. Thus, using the asymptotic results from the work of Marčenko and Pastur [9], we characterize the matrix $\mathbf{\Omega}$ as a Wishart matrix and thus the asymptotic density function of its eigenvalues, $f_{\mathbf{\Omega}}(\lambda)$, follows the well-known Marčenko-Pastur distribution:

$$f_{\mathbf{\Omega}}(\lambda) = \left(1 - \frac{1}{\alpha}\right)^+ \delta(\lambda) + \frac{\sqrt{(\lambda - \hat{\lambda}_{\text{min}})^+ \cdot (\hat{\lambda}_{\text{max}} - \lambda)^+}}{2\pi\alpha\lambda}, \tag{6}$$

where $\hat{\lambda}_{\text{min}} = (1-\sqrt{\alpha})^2$ and $\hat{\lambda}_{\text{max}} = (1+\sqrt{\alpha})^2$ are the support region boundaries of $f_{\mathbf{\Omega}}(\lambda)$ and $\alpha = \lim_{K,E\to 0} K/E$.

Surprisingly these results are excellent approximations even for quite small systems [10]. For the finite case, the real minimum and maximum eigenvalues of $\mathbf{\Omega}$, $\lambda_{\text{min}}$ and $\lambda_{\text{max}}$ can be estimated by $\hat{\lambda}_{\text{min}}$ and $\hat{\lambda}_{\text{max}}$ respectively since $\mathbb{E}[\lambda_{\{\text{min,max}\}}] = \hat{\lambda}_{\{\text{min,max}\}}$ with a speed of convergence $E^{-2/3}$ as it is detailed in [11]. To keep $\delta_K \in (0, 1)$, one needs to consider only the $\lambda_{\text{max}}$ since the $\lambda_{\text{min}}$ is always positive because $\mathbf{\Omega}$ is positive semidefinite by definition. Then $\lambda_{\text{max}}$ must obey:

$$\lambda_{\text{max}} < 1 + \delta_K < 2 \Longrightarrow (1 + \sqrt{K/E})^2 < 2. \tag{7}$$

Then, the condition for the ratio $K/E$, $\mathcal{C}_{\text{CS}}$, is given by

$$\mathcal{C}_{\text{CS}}: \quad K/E \;<\; (\sqrt{2} - 1)^2 = 0.1716. \tag{8}$$

Although one can think that even for the case of perfect channel estimation the required $E$ may become unpractical for high values of $K$, several more eavesdropping nodes may be required since $\mathcal{E}$ has access only to a contaminated version of the channel matrix $\tilde{\mathbf{\Phi}}$. This behavior is discussed further in the Numerical Results section.

### B. Eavesdropping in the Projection Phase

This phase is very robust against malicious and passive eavesdropping. Although an eavesdropper can have full access to the signal sent by the relays, i.e. $\mathbf{y}(n)$, to the fusion center (assuming that this signal is not encrypted), this signal is implicitly encoded using the MAC matrix $\mathbf{\Phi}$, and therefore the eavesdroppers cannot decode $\mathbf{x}_K(n)$ since they do not have access to $\mathbf{\Phi}$ [2].

Actually, this coding mechanism is not new and comes from the well-known discipline of *Network Coding* [12], where the signals from different sources are not handled individually and algebraic operations among them are allowed instead. So, sending linear combinations of the signals offers a natural way of protection [13]. Since this is one of the benefits of the Network Coding and it is already discussed in e.g. [13], we only focus on the robustness against eavesdropping on the *Sensing Phase*.

## IV. Numerical Results

The parameters that configure the basic setup of the simulations are as follows:

- Number of *sensing nodes*: $S = 200$.
- Number of *active sensors*: $K = 10$.
- Number of *relay nodes*: $R = 60$.
- Number of *eavesdropping nodes*: $E = [0, 110]$.
- Noise Power: $\sigma^2_{\mathbf{z}} = 0$. Although any real application measurement will be corrupted by at least a small amount of noise, we set $\sigma^2_{\mathbf{z}}$ to zero in order to better evaluate the system performance.

We also define the following figures of merit.

- *Channel estimation distortion*, $\mathcal{D}$. It measures the ratio in dB between the power of the estimation degradation $\sigma^2_{\mathbf{\Sigma}}$ and the variance of the channel coefficients $\sigma^2_{\mathbf{\Phi}}$, namely,

$$\mathcal{D} = 10 \log\left(\frac{\sigma^2_{\mathbf{\Sigma}}}{\sigma^2_{\mathbf{\Phi}}}\right). \tag{9}$$

- *Probability of recovery*. It measures the eavesdropper's reconstruction rate of $\mathbf{x}_K(n)$, i.e., $P(\hat{\mathbf{x}}_K(n) = \mathbf{x}_K(n))$ using $\mathcal{P}2$.

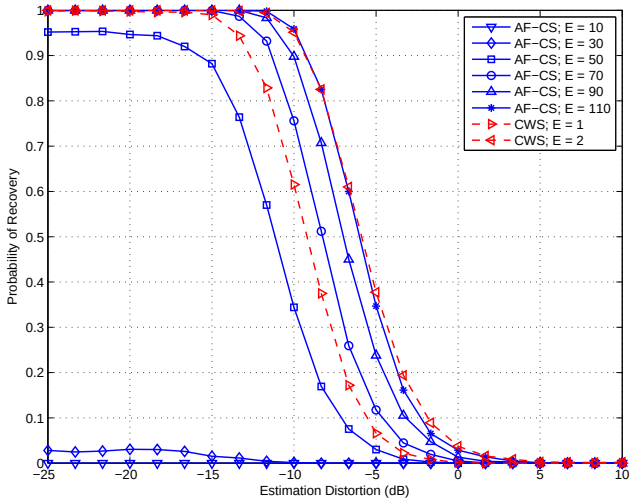


Fig. 2. Probability of recovery as a function of the channel estimation distortion for different number of coordinated eavesdroppers for $K = 10$ and $S = 200$. Solid lines represent the performance of AF-CS while dashed lines denote CWS. This figure has been averaged over 1000 realizations.

First, we study the probability of recovery as a function of the number of eavesdropping nodes using AF-CS. We observe in Fig. 2 that the set $\mathcal{E}$ can only decode the signal perfectly and with high probability for large values of $E$, i.e., when $E$ satisfies $\mathcal{C}_{\text{CS}}$. Moreover, we can observe that the AF-CS is perfectly secret for values of $E < K$. The values $E > K$ but below the condition $\mathcal{C}_{\text{CS}}$ can only decode the transmitted signal with low probability.

Second, Fig. 2 also shows that the robustness of AF-CS against eavesdropping increases rapidly with the channel estimation distortion. For instance, if the channel estimation error is 10 times smaller that the variance of the channel coefficients, i.e., $\sigma^2_{\mathbf{\Sigma}} = 0.1\ \sigma^2_{\mathbf{\Phi}}$, more than 110 eavesdropping nodes are required in order to recover the signal with high probability. Furthermore, for the case where the channel estimation error $\sigma^2_{\mathbf{\Sigma}}$ is of the same order than the variance of the channel coefficients $\sigma^2_{\mathbf{\Phi}}$ there is no configuration of $\mathcal{E}$ that recovers the signal with high probability.

Last, we compare our proposed AF-CS scheme with another distributed CS technique, the CWS in [4]. Although CWS has not been designed as a physical layer secure scheme, we assess its secrecy performance since this approach is one of the most extended CS approaches in the WSN literature and we compare both schemes in terms of physical layer secrecy performance. Simulation results show that a single eavesdropper with a channel distortion of less that $-15$dB suffices in decoding the transmitted signal with high probability. Furthermore, it can be seen in Fig. 2 that for the 110 eavesdroppers configuration, the AF-CS achieves the same performance as the CWS with only 2 eavesdroppers.

## V. Conclusions

In this paper, we have evaluated the *physical layer secrecy* of a *distributed compressed sensing* scheme based on amplify-and-forward relay configuration AF-CS against a *passive eavesdropper agent*, which is composed by several malicious and coordinated nodes. We have demonstrated that the system achieves perfect secrecy for a small number of eavesdropping nodes. For larger number of eavesdroppers we propose a design condition based on random matrix theory in order to guarantee perfect recovery of the transmitted signal with high probability. The simulation results support our claim, that is, the scheme under study is perfectly secret at physical layer when the number of eavesdropping nodes is below the sparsity level of the signal. On the other hand, and assuming perfect channel estimation, high decoding rates are only achievable when the number of eavesdroppers is large enough to hold the *restricted isometric property* condition. Moreover, we show that its robustness against passive eavesdropping increases rapidly when the eavesdroppers have degraded channel estimations. Furthermore, AF-CS drastically outperforms other compressed sensing solutions for wireless sensor networks in terms of the physical layer secrecy. The secrecy performance achieved by the scheme studied in this paper remains as an open issue.

## References


[1] D. L. Donoho, "Compressed Sensing," *Information Theory, IEEE Transactions on*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[2] Y. Rachlin and D. Baron, "The Secrecy of Compressed Sensing Measurements," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, Sep. 2008, pp. 813 –817.

[3] S. Agrawal and S. Vishwanath, "Secrecy using Compressive Sensing," in *Information Theory Workshop*, Paraty, Brazil, Oct. 2011.

[4] W. Bajwa, J. Haupt, A. Sayeed, and R. Nowak, "Compressive Wireless Sensing," in *Information Processing in Sensor Networks, 2006. IPSN 2006. The Fifth International Conference on*, 2006, pp. 134 –142.

[5] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Optimization of the Amplify-and-Forward in a Wireless Sensor Networks Using Compressed Sensing," in *Proc. 19th European Signal Processing Conference (EUSIPCO '11)*, Barcelona, Spain., Aug. 2011.

[6] X. Feng and Z. Zhang, "The Rank of a Random Matrix," *Applied Mathematics and Computation*, vol. 185, pp. 689–694, 2007.

[7] E. J. Candes and T. Tao, "Decoding by Linear Programming," *Information Theory, IEEE Transactions on*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[8] R. G. Baraniuk, M. A. Davenport, R. A. DeVore, and M. B. Wakin, "A Simple Proof of the Restricted Isometry Property for Random Matrices," *Constructive Approximation*, 2007.

[9] V. A. Marčenco and L. A. Pastur, "Distribution of Eigenvalues for Some Sets of Random Matrices," *Math USSR Sbornik*, vol. 1, pp. 457–483, 1967.

[10] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*, Foundations and Trends in Communications and Information Theory 1 (1), Jun. 2004.

[11] I. M. Johnstone, "On the Distribution of the Largest Eigenvalue in Principal Components Analysis," *Ann. Statist.*, vol. 29, no. 2, pp. 295–327, 2001.

[12] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Network Coding Theory*, now Publishers, 2005.

[13] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*, now Publishers, 2007.