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

Joan Enric Barceló-Lladó, Antoni Morell, and Gonzalo Seco-Granados, *Senior Member, IEEE*

***Abstract*— In this paper, we assess the physical-layer secrecy performance of the amplify-and-forward compressed sensing (AF-CS) framework when malicious eavesdropping nodes are listening. In particular, we investigate the robustness of the AF-CS scheme in the presence of a group of coordinated eavesdropping nodes under the assumption that they have corrupted channel state information. In order to fulfil this assumption, we propose a channel estimation technique based on pseudorandom pilots. This technique introduces extra uncertainty only in the channel estimation of the eavesdroppers. Our simulation results evaluate the physical-layer protection as a function of the total number of coordinated eavesdroppers and the level of channel estimation distortion of the eavesdroppers. We demonstrate that a small number of eavesdroppers (small being defined later on) has a zero probability of recovering the intended signal. We also show that a very large number of eavesdropping nodes are required to perfectly recover the signal in comparison with other distributed compressed sensing schemes in the literature.**

***Index Terms*— Communication system security, compressed sensing, physical layer, wireless sensor networks.**

I. Introduction

A. Physical-Layer Secrecy Background

Physical-Layer security proposes different mechanisms in order to protect the wireless communication against mainly malicious jammers [1], [2], and/or unauthorized eavesdroppers. We address the latter case, and throughout this document, this case is referred to as Physical-Layer (PHY-layer) secrecy. Therefore, the basic aim of the PHY-layer secrecy is to allow reliable transmission of confidential messages over a wireless link in presence of eavesdroppers.

This issue has been traditionally addressed using spread spectrum techniques such as Code Division Multiple Access (CDMA). Thanks to the pseudorandom codes that can be seen as secret keys, the intended signal is converted in a noise-like signal for any receiver that does not possess the code. However and generally speaking, CDMA has the limitation of short keywords (about 24 bits [3]) and a persistent eavesdropper could get the key with some little effort. That is why upper-layer cryptographic techniques have been used so far. These techniques assume large keys that make the message almost impossible to decipher. However, cryptographic mechanisms have two main problems in the wireless scenario: first, the distribution of the key over a public medium, and second, the high computational complexity, which goes beyond the hardware and power limitations of some devices such as in Wireless Sensor Networks (WSNs).

For these reasons and according to the proliferation of wireless communications, the interest on secrecy mechanisms at physical layer has dramatically grown in the last decade. However, this concept is not new in the literature and comes from 1949, when Shannon postulated the foundations of the modern cryptography in his seminal work [4]. The proposed scheme assumes that a transmitter sends encrypted information using a non-reusable key over a noiseless channel and with the presence of an eavesdropper that has access to the transmit coding scheme and the transmitted signal. In that paper, the author postulates the conditions that the code must satisfy in order to ensure perfect secrecy. This work opened a whole branch of key-based secrecy research.

Later in the seventies, Wyner opened a new branch of research about keyless secrecy techniques in [5]. In particular, the author assumes that the eavesdropper has the additional effect of the non-ideal wiretap channel [6], which can be seen as a degradation of the main channel. Under this assumption, it obtains the maximum rate over the main channel that assures a negligible amount of information in the wiretap channel.

One of the common ways to protect the intended message against eavesdropping is to use opportunistic transmissions deliberately scheduled when the wiretap channel fades [7]. It is then possible to obtain reliable transmissions even when the eavesdropper experiments a better average SNR than the legitimate receiver [8]. This approach can be extended to a general MIMO scenario, where the transmitter adds a precoding matrix orthogonal to the wiretap channel matrix [9].

These techniques require a perfect knowledge of the *Eavesdropper Channel State Information* (ECSI). Actually, relatively fewer studies consider the case of a complete absence of ECSI at the intended pair transmitter-receiver. However, other works require only the knowledge of the statistics of the wiretap channel [10], [11]. They use an artificial noise injected to the signal in order to degrade the quality of the wiretap channel. Moreover, the authors of [12] show the poor performance of waterfilling techniques when no information about the eavesdropper channel is available.

Manuscript received June 9, 2013; revised November 9, 2013, January 31, 2014, and February 8, 2014; accepted February 21, 2014. Date of publication March 5, 2014; date of current version April 15, 2014. This work was supported by the Spanish Research and Development Project TEC2011-28219. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Y.-W. Peter Hong.

The authors are with the Telecommunications and Systems Engineering Department, Universitat Autònoma de Barcelona, Barcelona 08193, Spain (e-mail: joanenric.barcelo@uab.es; antoni.morell@uab.es; gonzalo.seco@uab.es).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2014.2309855

Many other studies regarding different network configurations are also being actively studied, contributing with new alternatives and having different performances from the point of view of secrecy. For the subsequent works, the interested reader may find an excellent review about PHY-layer secrecy in [12]. We do not review these other exciting activities, but focus our attention on the secrecy schemes that we can build using Compressed Sensing (CS) strategies, specially when applied to WSNs. The interested reader can find in Section II next a brief discussion about how compressed sensing techniques can be advantageous from the PHY-layer secrecy perspective and also a review on the applications of CS in WSNs. We anticipate that none of the existing solutions provides a high degree of PHY-Layer protection since they do not guarantee a secure key transmission (see Section II.B) and the signal can be decoded with high probability by only one eavesdropper (see the simulation results in Section VI). Therefore, this paper proposes an alternative scheme and we assess its performance from the point of view of PHY-layer secrecy.

B. Contributions and Structure of the Paper

In this paper, we propose the AF-CS framework as a distributed and secret CS scheme. AF-CS was first introduced in [13] and detailed in [14] as an original contribution of the authors. We have shown that it is able to reduce the energy consumption using, at the same time, a very limited number of channel uses.

We address the secrecy level of the AF-CS scheme in the presence of not only one but a group of coordinated and passive eavesdroppers with corrupted channel state information. In order to provide the so-called PHY-layer secrecy, the system takes advantage of the linear combinations that are produced on the air thanks to the particular Multiple Access Channel (MAC) proposed in our AF-CS scheme. In order to corrupt the estimation of the wiretap channel matrix of the eavesdroppers, we also propose two secure channel estimation techniques based on pseudorandom pilots that allow the system to control the distortion introduced to the channel estimate of the eavesdroppers and hence to guarantee a desired secrecy level. These strategies are similar to the artificial noise injection technique proposed in [10] and [11], but with the main difference that the noise is not used to encode or mask the signal but only the pilots in the channel estimation. Doing so, the energy consumption is reduced in comparison to the artificial noise injection method. Moreover, the second proposed technique overcomes the problem of generating and transmitting a pseudo-random sequence securely by exploiting the reciprocity of the wireless channel. This approach has been studied in the literature in [15]–[17] for MIMO scenarios.

Finally, we evaluate the secrecy performance of our proposed AF-CS framework in numerical simulations and we compare it with Compressive Wireless Sensing CWS-like schemes [18]. We find out that AF-CS dramatically increases the protection against eavesdropping at physical layer.

The rest of the paper is organized as follows. In Section II we revise the works in the literature related to compressed sensing as a physical layer secret solution, the strategies proposed in WSNs, and the improvements achieved with our proposed scheme. In Section III we present the problem statement and the assumptions considered throughout the paper. Section IV is the main contribution of our paper and analyzes the secrecy properties of the AF-CS scheme. The random pilot techniques that control the CSI at the eavesdroppers are introduced in Section V. Simulation results are given in Section VI and conclusions are drawn in Section VII.

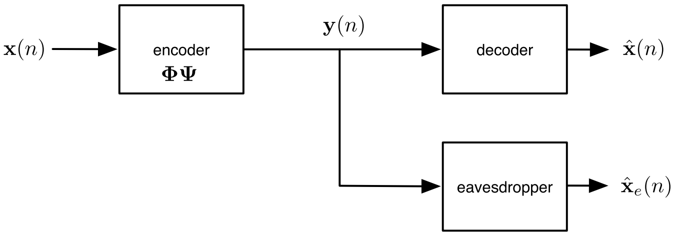

Fig. 1. Block diagram of the key-based PHY-Layer secrecy scenario.

C. 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 conjugate transpose (Hermitian) respectively. $[\mathbf{X}]_{i,j}$, $[\mathbf{x}]_i$ is the (ith, jth) element of matrix $\mathbf{X}$, and ith position of vector $\mathbf{x}$, respectively. $[\mathbf{X}]_i$ is a row vector that contains the ith row of $\mathbf{X}$. $(\cdot)^\star$ denotes the optimal value. 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. The notation $\|\mathbf{A}\|$ indicates the Frobenius norm of a matrix $\mathbf{A}$. $\mathbb{E}[\cdot]$ is the statistical expectation. $\mathcal{N}(\boldsymbol{\mu}, \mathbf{R})$ is a Gaussian vector distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\mathbf{R}$, $\sigma_{\mathbf{x}}^2$ is the variance of $\mathbf{x}$. The notation $\hat{x}$ denotes the estimation of the scalar x. The symbol $\backslash$ denotes set subtraction, i.e., $\mathcal{A}\backslash\mathcal{B}$ removes to the set $\mathcal{A}$ the elements belonging to the set $\mathcal{B}$.

II. Related Work

A. Compressed Sensing as a PHY-Layer Secret Strategy

Compressed Sensing is a novel tool that allows us to sample the signals below the Nyquist rate [19], 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 (the interested reader is encouraged to visit the Rice's CS database at dsp.rice.edu/cs). However, only a very few works relate CS with secrecy. In fact the most relevant contributions up to date are collected in the following four references: [20] and [21] for the key-based secrecy case, and [22] and [23] for the keyless secrecy case.

The contributions in [20] and [21] consider the scenario in Fig. 1, with one source, one receiver, and one eavesdropper. The product of the transform matrix and the sensing matrix, i.e., $\mathbf{\Phi\Psi}$ can be seen as an encryption key, which is assumed to be unknown by the eavesdropper.

Thus, the eavesdropper receives an exact copy of the transformed measurements, i.e.,

$$\mathbf{y}(n) = \mathbf{\Phi\Psi x}(n). \tag{1}$$

Therefore, the paper studies how difficult it is for the eavesdropper to recover $\mathbf{x}(n)$ from the measurements $\mathbf{y}(n)$ without

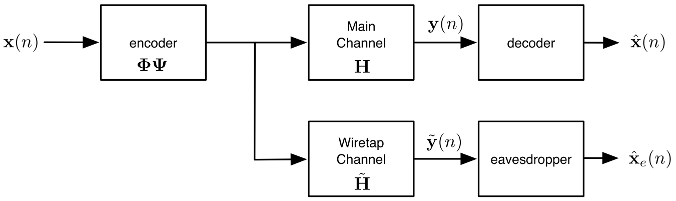

Fig. 2. Block diagram of the keyless PHY-Layer secrecy scenario.

the knowledge of the key $\mathbf{\Phi\Psi}$. Actually, they proved (see Lemma 1 in [20]) that compressed sensing encryption does not achieve perfect secrecy, i.e., $I\,(\mathbf{x}(n); \mathbf{y}(n)) > 0$. The mutual information would be zero if and only if $\mathbf{x}(n)$ and $\mathbf{y}(n)$ are independent. However, since $\mathbf{\Phi\Psi}$ is linear, $\mathbf{x}(n) = \mathbf{0}$ implies that $\mathbf{y}(n) = \mathbf{0}$, and hence $P(\mathbf{y}(n) = \mathbf{0}|\mathbf{x}(n) = \mathbf{0}) \neq P(\mathbf{y}(n) = \mathbf{0})$, meaning statistical dependence.

Furthermore, the authors in [20] introduce the concept of Computational Secrecy. It is applied to the cases when the encrypted data contains complete information about the message but extracting this information will be equivalent to solve a computational problem (NP-hard discovery). According to that definition, they proved that the eavesdropper cannot reconstruct the message using a different (wrong) key $\mathbf{\Phi}'\mathbf{\Psi}'$ with probability one, for the case when $\mathbf{\Phi\Psi}$ and $\mathbf{\Phi}'\mathbf{\Psi}'$ are independent.

The work in [21] extends the results in [20] and considers the perfect secrecy problem using CS. They show that under certain conditions, perfect secrecy via CS is achievable. The conditions are: i) the signal $\mathbf{x}(n)$ has a uniform distribution over a given alphabet; ii) the key $\mathbf{\Phi\Psi}$ is $R \times S$, where R is the number of measurements, S is the dimension of the signal $\mathbf{x}(n)$, and K is the number of nonzero values (sparsity level) of $\mathbf{x}(n)$. Thus, the condition $R > 2K$ is imposed; iii) the matrix $\mathbf{\Phi}$ holds *Restricted Isometry Property* (RIP) [24]; iv) the number of source messages goes to infinity; and v) the null message does not exist, i.e., $\mathbf{x}(n) \neq \mathbf{0}$.

On the other hand, the scenario in Fig. 2 is considered in [22] and [23]. This scenario is different than the one in Fig. 1 because i) the CS encoding matrix $\mathbf{\Phi\Psi}$ is also known by the eavesdropper, and ii) they consider different channels for the legitimate user (main channel) and the eavesdropper (wiretap channel). The signal model is thus:

$$\mathbf{y}(n) = \mathbf{H\Phi\Psi x}(n) + \mathbf{w}(n) \tag{2}$$

for the legitimate user, and

$$\tilde{\mathbf{y}}(n) = \tilde{\mathbf{H}}\mathbf{\Phi\Psi x}(n) + \tilde{\mathbf{w}}(n) \tag{3}$$

for the eavesdropper, where $\mathbf{H} \in \mathbb{R}^{S\times S}$ and $\tilde{\mathbf{H}} \in \mathbb{R}^{S\times S}$ are the main and the wiretap (flat-fading) channel matrices respectively, and $\mathbf{w}(n)$ and $\tilde{\mathbf{w}}(n)$ model the Additive White Gaussian Noise (AWGN) of the wireless channels, both distributed as $\mathcal{N}(0, \sigma_{\mathbf{w}}^2)$

Differently from [20], the authors in [22] do not focus on either perfect secrecy or computational secrecy. They introduce the concept of *Wolfowitz* secrecy, which states that the eavesdropper is unable to decode the message with high probability, or equivalently, that the eavesdropper's Probability of Recovery can be made arbitrarily small. So, it lies between perfect secrecy and computational secrecy.

The authors demonstrated that it is possible to ensure Wolfowitz secrecy if the average singular value of $\tilde{\mathbf{H}}$ is less than a given constant multiple of the minimum singular value of $\mathbf{H}$.

In the same line, the authors in [23] study the secrecy capacity [25] of the wiretap channel in Fig. 2 when CS-like matrices are using to encode the message.

B. PHY-Layer Secrecy Using Compressed Sensing in WSNs

According to the references cited in the previous subsection, CS postulates as a good candidate in order to provide PHY-layer secrecy against eavesdropping in addition to the other CS benefits.

However, the scenario considered by the authors is a point-to-point communication that involves only a single transmitter who compresses the signal, one receiver and one eavesdropper. Hence, this scenario follows a centralized approach that is not directly applicable to our scenario due to the decentralized nature of the WSN environment. These limitations are addressed in [14] and can be summarized as follows:

- If the signal $\boldsymbol{\omega}(n) = \mathbf{\Psi x}(n)$ is not purely sparse, the CS encoding cannot be directly applied in a decentralized approach, since the K-largest coefficients of $\boldsymbol{\omega}(n)$ have to be selected first.
- High energy consumption and channel uses per measurement are required.

In order to overcome these problems, a Compressive Wireless Sensing (CWS)-like approaches can be proposed [18]. Although these are designed to deal with energy-efficient communications, it is meaningful to examine them from a PHY-layer secrecy perspective as well. In this case, two main issues have to be taken into account:

- The CS matrix coefficients, which act as the key, have to be securely sent over the wireless channel somehow.
- The CS matrix coefficients cannot be easily deduced from the measurements. To extract these coefficients from a small subset of measurements, the authors in [26] propose an algorithm that allows to discover the CS matrix from only a few measurements when the matrix has some predefined structure, e.g., Fourier matrix, Discrete Cosine Transform (DCT) matrix, Toeplitz matrix, etc. Therefore, the CS matrix design is an issue since the usual matrices are not valid for secrecy purposes.

In conclusion, the current PHY-Layer secure CS schemes do not suit for decentralized scenarios. Moreover, the current distributed CS techniques are not designed to provide PHY-Layer secrecy. Hence, new CS schemes are needed in order to implement secret systems in WSNs.

On one hand, in this paper we take a new approach where the channel matrix is used as the CS matrix and it can be seen as the encryption key of the PHY-layer secrecy scheme following the key-based approach in [20] and [21]. On the other hand, we also consider the case where the eavesdroppers suffer from the effect of the wiretap channel as in [22] and [23], and in particular, they work with a degraded version of the channel matrix.

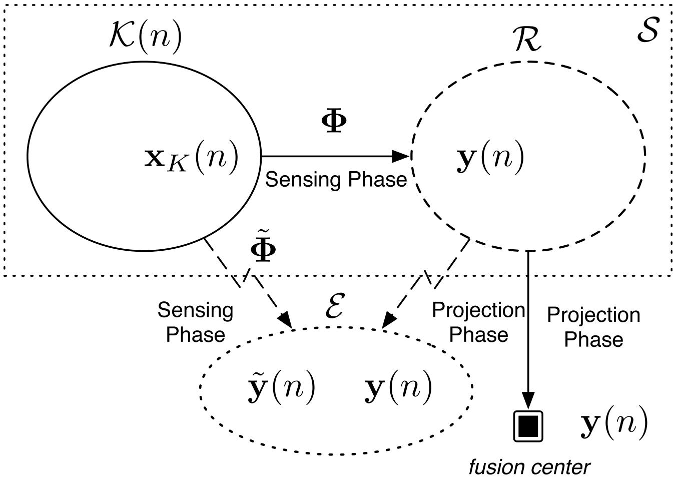

Fig. 3. Multiple active channel scenario composed by K active sensing nodes, R relay nodes, E eavesdropping nodes, and one fusion center.

Actually, our approach cannot be classified as either a key-based or a keyless approach. Instead, it follows a more general scheme that can be seen as a combination of both approaches. The subsequent advantages and contributions with respect to each of the approaches are listed next.

Key-based PHY-secrecy. One of the challenges in key-based schemes is to securely exchange the key matrices. In AF-CS, there is no exchange of CS matrix since the sensing nodes do not need the matrix to encode the message. Instead, the encoding is performed on the air. It reduces the computational complexity derived from the encryption process. Hence, it has a great impact on the design of the WSNs because the sensing nodes are very hardware limited.

Keyless PHY-secrecy. Although we consider that both the intended and the wiretap communications are perturbed by the wireless channel, we do not assume any knowledge of the wiretap channel by the intended nodes. As it is said in [12], very few works in the literature consider the case of no ECSI at either the transmitter or the intended receiver.

III. System Model and Assumptions

A. Description of the AF-CS Framework

We consider a WSN 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 Fig. 3, that is:

- A set $\mathcal{S}$ of S sensing nodes connected (wirelessly) to one fusion center, that acts as the intended receiver. 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 Amplify-and-Forward (AF) mode.
- A set $\mathcal{E}$ (of cardinality E) of malicious and passive eavesdropping nodes.

According to the CS nomenclature, K also corresponds to the number of nonzero elements of the transmitted vector $\mathbf{x}(n) \in \mathbb{R}^S$, and R is the number of measurements used in the reconstruction at the fusion center, i.e., the number of rows of the sensing matrix, $\mathbf{\Phi} \in \mathbb{R}^{R\times S}$, where typically $K < R < S$. On the contrary, the eavesdroppers use E measurements to try to decode the signal, i.e., the number of rows of the sensing matrix, $\tilde{\mathbf{\Phi}} \in \mathbb{R}^{E\times S}$, used by the eavesdroppers.

B. Assumptions

We assume perfect Channel State Information (CSI) at the fusion center for all the links that go from any sensing node to a relay node in $\mathcal{R}$. In particular, we assume that the channel matrix, also referred to as the sensing matrix $\mathbf{\Phi} \in \mathbb{R}^{R\times S}$ (see Fig. 3) follows the Gaussian measurement ensemble, where:

$$[\mathbf{\Phi}]_{i,j} \sim \mathcal{N}(0, R^{-1}). \tag{4}$$

The variance of the sensing matrix R^{-1} is a convention in the literature in order to maintain the relation

$$\mathbb{E}\left[\|\mathbf{\Phi}\mathbf{x}\|\right] = \mathbb{E}\left[\|\mathbf{x}\|\right] \tag{5}$$

for an arbitrary vector $\mathbf{x}$. This assumption is just for convenience and it does not affect to the generality of the model since the channel gain can be adjusted at the receiver if needed. Furthermore we assume that the RIP condition [27] holds for the channel matrix $\mathbf{\Phi}$ with the selected values of K and S. In other words, we assume that the legitimate receiver is able to perfectly recover the intended message in the noiseless case or with bounded error in general [28].

On the other side, we assume partial knowledge of the CSI at the eavesdroppers for all the links that go from any sensing node to a relay node in $\mathcal{R}$. The wiretap channel matrix, also referred to as wiretap sensing matrix $\tilde{\mathbf{\Phi}} \in \mathbb{R}^{E\times S}$ (see Fig. 3) follows the Gaussian measurement ensemble, where:

$$[\tilde{\mathbf{\Phi}}]_{i,j} \sim \mathcal{N}(0, E^{-1}). \tag{6}$$

However, there is no mutual channel knowledge in the sense that the eavesdroppers do not have access to $\mathbf{\Phi}$, and that the fusion center does not need to know $\tilde{\mathbf{\Phi}}$. Therefore, the typical assumption of perfect or partial ECSI at the intended receiver is relaxed.

Moreover, we make no assumptions regarding the links from $\mathcal{R}$ to the fusion center other than these links are controlled by a certain orthogonal policy that requires R channel uses for each sample time n in order to transmit the data from the relays to the fusion center.

Finally, we assume that neither the intended receiver nor the eavesdroppers have any prior knowledge about the signal of interest.

C. Figures of Merit

In order to quantify the level of secrecy of the proposed AF-CS scheme, we study the following figures of merit between the original message $\mathbf{x}$ and the decoded message $\hat{\mathbf{x}}$.

- *Probability of Recovery*, PoR $= P(\mathbf{x} = \hat{\mathbf{x}})$. It measures the probability that the eavesdroppers succeed in recovering the original signal $\mathbf{x}$. We also define the Zero-Probability of Recovery (ZPoR) when the eavesdroppers decode the signal with null probability. Note that

Wolfowitz Secrecy [22] is achieved when the PoR can be made arbitrarily small and also that ZPoR is even stronger than Wolfowitz Secrecy.

- *Wiretap Distortion*. It measures the normalized squared error of the eavesdropper decoded signal with respect to the intended one, i.e.,

$$\mathcal{D}_e = \mathbb{E}\left[\frac{\|\mathbf{x}-\hat{\mathbf{x}}\|^2}{\|\hat{\mathbf{x}}\|^2}\right]. \tag{7}$$

Other common metrics in the literature are: *Perfect Secrecy* [21], *Computational Secrecy* [20], *Wolfowitz Secrecy* [22], *Equivocation Rate* [29], *Secrecy Rate* [30], and *Secrecy Capacity* [25].

IV. Eavesdropping the Amplify-and-Forward Compressed Sensing Scheme

In this paper, we consider the following three phases in the transmission of the sensor readings to the fusion center.

1) *Sensing phase*. In this phase K sensor readings are broadcasted time-synchronized and using uncoded transmissions to the relay nodes. In the context of the Amplify-and-Forward Compressed Sensing (AF-CS) scheme derived in the authors' work in [13] and [14], the K sensor readings to be transmitted are distributively selected taking into account linear predictions computed with past readings. The goal is to transmit only when the sensor readings change in a certain predefined quantity with the aim of saving energy. Note however that the results in this work are not restricted to the strategy used in [14] to select sensor readings in transmission and recover them later at the sink node.
2) *Projection phase*. Each relay has received linear combinations of $\mathbf{x}_K(n)$ due to the on-air addition of the transmitted radio waves, modeled by the sensing matrix $\mathbf{\Phi}$. Then, it relays to the fusion center using a given orthogonal transmission (e.g., time multiplexing).
3) *Reconstruction phase*. The objective is to recover the sparse vector $\mathbf{x}_K(n)$ from the measurements of the projection vector $\mathbf{y}(n)$. The original decoder $\mathcal{P}0$ directly enforces sparsity on the recovered vector by solving:

$$\begin{aligned}\mathcal{P}0: \quad & \underset{\hat{\mathbf{x}}_K(n)\in\mathbb{R}^S}{\text{minimize}} \quad \|\hat{\mathbf{x}}_K(n)\|_0 \\ & \text{subject to} \quad \mathbf{y}(n) = \mathbf{\Phi}\hat{\mathbf{x}}_K(n)\end{aligned} \tag{8}$$

where the l_0 (pseudo)norm is defined as $\|\mathbf{x}\|_0 = |\{x_i \neq 0\}|$, i.e., the number of non-zero entries in a vector $\mathbf{x}$. The main problem is that solving $\mathcal{P}0$ is a hard combinatorial problem and computationally intractable in the general case [19].

Alternatively, we propose to use a very usual approach in the literature, which is to relax $\mathcal{P}0$ by using the l_1 norm. Therefore, the fusion center computes the following linear program in the noiseless case

$$\begin{aligned}\mathcal{P}1: \quad & \underset{\hat{\mathbf{x}}_K(n)\in\mathbb{R}^S}{\text{minimize}} \quad \|\hat{\mathbf{x}}_K(n)\|_1 \\ & \text{subject to} \quad \mathbf{y}(n) = \mathbf{\Phi}\hat{\mathbf{x}}_K(n)\end{aligned} \tag{9}$$

The conditions when $\mathcal{P}1$ is equivalent to $\mathcal{P}0$ can be found in [28]. For the noisy case, the fusion center solves

$$\begin{aligned}\mathcal{P}2: \quad & \underset{\hat{\mathbf{x}}_K(n)\in\mathbb{R}^S}{\text{minimize}} \quad \|\hat{\mathbf{x}}_K(n)\|_1 \\ & \text{subject to} \quad \|\mathbf{y}(n) - \mathbf{\Phi}\hat{\mathbf{x}}_K(n)\|_2 < \varepsilon,\end{aligned} \tag{10}$$

where ε is an upper bound on the magnitude of the noise. Afterwards, the fusion center completes the remaining Q entries of the vector $\mathbf{x}(n)$, for example using linear prediction in the case of [14].

Next, we assess the PHY-layer secrecy performance of the sensing and projection phases. Note that the reconstruction phase is out of the scope of this paper because wireless transmissions are involved only in the first two phases.

A. Eavesdropping During the Sensing Phase

During this phase, 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,

$$\mathbf{y}(n) = \mathbf{\Phi}\mathbf{x}_K(n) + \mathbf{w}(n), \tag{11}$$

where the vector $\mathbf{y}(n) \in \mathbb{R}^R$ stacks all the received signals of the nodes in $\mathcal{R}$, the sensing matrix $\mathbf{\Phi}$ models the channel between $\mathcal{S}$ and $\mathcal{R}$ as a random matrix with i.i.d. Gaussian entries with zero mean and variance $\sigma^2_{\mathbf{\Phi}} = R^{-1}$. Finally, $\mathbf{w}(n)$ denotes white Gaussian noise with zero mean and variance $\sigma^2_{\mathbf{w}}$.

Similarly to (11), the signal at the eavesdroppers is

$$\tilde{\mathbf{y}}(n) = \tilde{\mathbf{\Phi}}\mathbf{x}_K(n) + \tilde{\mathbf{w}}(n) \tag{12}$$

where $\tilde{\mathbf{y}}(n) \in \mathbb{R}^E$ stacks the signals received by the nodes in $\mathcal{E}$, and $\tilde{\mathbf{\Phi}}$ models the channel between $\mathcal{S}$ and $\mathcal{E}$ as a random matrix with i.i.d. Gaussian entries with zero mean and variance $\sigma^2_{\tilde{\mathbf{\Phi}}} = E^{-1}$ and $\tilde{\mathbf{w}}(n)$ denotes white Gaussian noise with zero mean and variance $\sigma^2_{\tilde{\mathbf{w}}}$.

In the following, we focus on the noiseless case (i.e., $\sigma^2_{\tilde{\mathbf{w}}} = 0$) because it implies a worst-case condition in terms of secrecy performance of the AF-CS scheme, that is, signal reconstruction at the eavesdroppers can only be penalized with the presence of thermal noise. Fig. 4 supports this by showing the simulated operating wiretap distortion as a function of the SNR using in this case a network with $S = 200$, $K = 10$ and $E = [60, 70, 80, 90]$. Note in this case that the wiretap distortion decreases rapidly with SNR, being less than 10% of the power of the signal for SNR values around 10 dB.

Fixed $\sigma^2_{\tilde{\mathbf{w}}} = 0$, we consider in what follows two different cases: i) PHY-Layer secrecy with perfect CSI at the eavesdroppers, and ii) PHY-Layer secrecy with imperfect CSI.

1) Eavesdroppers With perfect CSI: Here, we assume that the eavesdroppers have perfect knowledge of the wiretap sensing matrix $\tilde{\mathbf{\Phi}}$. Then, the eavesdroppers would have to jointly solve $\mathcal{P}1$. The most common way to address its performance is by means of the Restricted Isometric Property (RIP). We reproduce it here using the new nomenclature for the eavesdropper set as:

Definition 1: [31]: *A matrix* $\tilde{\mathbf{\Phi}}$ *satisfies the RIP of order* K *with restricted isometry constant* $\delta_K \in (0, 1)$ *if*

$$(1-\delta_K)\|\mathbf{x}\|_2^2 \le \|\tilde{\mathbf{\Phi}}\mathbf{x}\|_2^2 \le (1+\delta_K)\|\mathbf{x}\|_2^2, \tag{13}$$

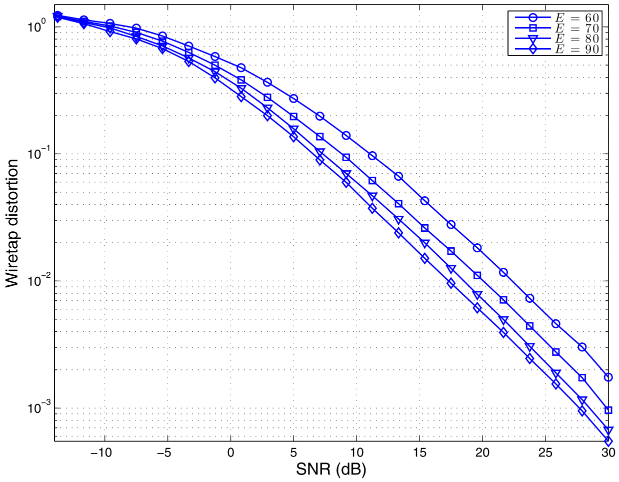

Fig. 4. Wiretap distortion as a function of the SNR (dB). The parameters of the simulation are: $S = 200$, $K = 10$, $E = [60, 70, 80, 90]$ (the condition $\mathcal{C}_{\text{CS}}$ in (14) holds). The decoder used is $\mathcal{P}2$. This figure has been averaged 1000 times.

where $\tilde{\mathbf{\Phi}}_K \in \mathbb{R}^{E\times K}$ *is formed by retaining any set of* K *or less columns from* $\tilde{\mathbf{\Phi}}$*,* $\mathbf{x}$ *is any* K*-sparse vector of the appropriate size, and* δ_K *is the smallest number (and not too close to one) that holds the RIP condition for each integer* $K = 1, 2, ...$

Most of the CS literature agree that if the elements of the matrix $\tilde{\mathbf{\Phi}}$ are selected from an i.i.d. Gaussian measurement ensemble (as in (6)), then $\tilde{\mathbf{\Phi}}$ will satisfy the RIP with overwhelming probability for $E \geq C_0 K \log S$ [28] or even $E \geq C_0 K \log(S/K)$ [19], [27], where C_0 is some positive constant. In addition to this already-existing results in the literature, the authors have incorporated a new relation in [14], which is

$$\mathcal{C}_{\text{CS}}: \quad E > K + K \log\left(\frac{S}{K}\right) \tag{14}$$

and better fits the experimental results. Without loss of generality, we will use $\mathcal{C}_{\text{CS}}$ as the CS condition in order to determine if $\mathbf{x}_K(n)$ can be recovered from $\tilde{\mathbf{y}}(n)$ with high probability or not.

Although it is very difficult to predict what happens when $E \sim K+K\log(S/K)$ [32], we will differentiate three possible cases for E: i) low values of E, i.e., $E \leq K$, ii) moderate values of E, i.e., $K < E \leq K + K\log(S/K)$, and iii) high values of E, i.e., $E > K + K\log(S/K)$, or what is the same, that E satisfies $\mathcal{C}_{\text{CS}}$.

For low values of E, we address the PHY-layer secrecy of the sensing phase with $E \leq K$ throughout the following lemmas.

Lemma 1: Let $\mathcal{X}'_E$ *denote the solution set of the eavesdroppers that is composed of all the possible recovered vectors at the eavesdropper's decoder for a received* $\tilde{\mathbf{y}}(n)$*. Hence, the cardinality of* $\mathcal{X}'_E$ *is at least*

$$M = \binom{S}{E} = \frac{S!}{(S-E)!E!}, \tag{15}$$

which means that the solution is not unique.

Proof During the proof of this lemma, we use the original decoder $\mathcal{P}0$. Let us remark that using $\mathcal{P}0$ in this lemma does not imply that we force the eavesdroppers or any node in the AF-CS scheme to use $\mathcal{P}0$ as the decoding strategy. On the contrary, we argue that the exact recovery conditions of $\mathcal{P}0$ are milder than in $\mathcal{P}1$ [28], and consequently: i) perfect recovery with $\mathcal{P}1$ guarantees perfect recovery with $\mathcal{P}0$ and ii) Zero-Probability of Recovery with $\mathcal{P}0$ ensures Zero-Probability of Recovery with $\mathcal{P}1$.

In order to show that the solution is not unique, it suffices to prove that there exists at least one E-sparse vector $\mathbf{x}_E$ with loaded entries according to any subset of indices $\mathbf{\Omega}_E \subset \mathcal{S}$ of cardinality E. Therefore, let the matrix $\tilde{\mathbf{\Phi}}_{\mathbf{\Omega}_E}$ denote a $E \times E$ measurement matrix obtained by selecting the E columns of $\tilde{\mathbf{\Phi}}$ corresponding to the indices $\mathbf{\Omega}_E$ and let the E-dimensional vector $\mathbf{x}_{\mathbf{\Omega}_E}$ collect the E loaded entries of $\mathbf{x}_E$. It is verified that

$$\mathbf{y}(n) = \tilde{\mathbf{\Phi}}_{\mathbf{\Omega}_E}\mathbf{x}_{\mathbf{\Omega}_E} \tag{16}$$

for any $\mathbf{\Omega}_E$. Since the matrix $\tilde{\mathbf{\Phi}}_{\mathbf{\Omega}_E}$ is full rank with overwhelming probability, a vector $\mathbf{x}_{\mathbf{\Omega}_E} = \tilde{\mathbf{\Phi}}^{-1}_{\mathbf{\Omega}_E}\tilde{\mathbf{y}}(n)$ exists for any $\mathbf{\Omega}_E$.

Since a number of

$$M = \binom{S}{E} = \frac{S!}{(S-E)!E!}, \tag{17}$$

different index sets of E elements over the set $\mathcal{S}$ can be generated, the proof of Lemma 1 is concluded.

Lemma 2: If $E < K$*, the eavesdroppers will recover the signal* $\mathbf{x}_K(n)$ *with* zero-probability*, which is defined as*

$$P(\hat{\mathbf{x}}_K(n) = \mathbf{x}_K(n)) = 0. \tag{18}$$

Moreover, if $E = K$*, the eavesdroppers will recover the original vector* $\mathbf{x}_K(n)$ *with* nonzero-probability*. However, it is asymptotically zero in S.*

Proof For the case $E < K$, the rank of $\tilde{\mathbf{\Phi}}$ is $\text{rank}(\mathbf{\Phi}) = E$ with overwhelming probability [33], and thus the sparsity on the reconstruction of $\mathbf{x}_K(n)$ cannot be higher than an E-sparse signal (instead of K-sparse) [20].

For the case $E = K$, let the vector $\mathbf{x}_K(n)$ be in the solution set $\mathcal{X}'_E$ (with cardinality M). Therefore, there is a probability of selecting it among all other possible solutions. Since all the vectors in $\mathcal{X}'_E$ minimize the utility function and satisfy the constraints in the same way, the decoder does no have any extra information to prioritize $\mathbf{x}_K(n)$ in front of the other $M-1$ possible solutions. According to this, we assume that the decoder $\mathcal{P}0$ randomly selects one vector among the possible solution set $\mathcal{X}'_E$. Hence:

$$P(\mathbf{x}_K(n) = \mathbf{x}) = \frac{1}{M}, \tag{19}$$

where M was given in (15). Thus,

$$P(\mathbf{x}_K(n) = \mathbf{x}) = \frac{(S-K)!K!}{S!}. \tag{20}$$

In the asymptotic regime we have

$$\lim_{S\to\infty} \frac{K!(S-K)!}{S!} = 0. \tag{21}$$

This asymptotic result makes sense in real scenarios since $S \gg K$ is typically assumed in CS schemes. For a given K, the Probability of Recovery decreases quickly as S increases.

Actually, even for small ratios of S/K the Probability of Recovery is almost negligible.

For moderate values of E, Zero-Probability of Recovery cannot be guaranteed for the case $E > K$ with perfect CSI. Note that $\mathcal{C}_{\text{CS}}$ is not satisfied and hence perfect signal recovery is not guaranteed although it may happen in some cases. Furthermore, since E does not satisfy $E < K$, the previous ZPoR situation is no longer verified. Roughly speaking, we have no condition that sustains either ZPoR or perfect recovery. However experimentation reveals some quite intuitive behavior, consisting in that the closer E is to the condition $\mathcal{C}_{\text{CS}}$ (i.e., the bigger E is), the higher the PoR will be. Additionally, note that even if $\mathbf{x}_K(n)$ is successfully decoded, it contains a small amount of the sensor readings in any case since the condition $S \gg K$ holds. Thus, the remaining $Q = S - K$ measurements still have to be predicted. If the prediction uses past readings (both received and predicted), such it is the case in [14], then the current prediction is compromised by erroneous past decodings.

For high values of E, if the condition $\mathcal{C}_{\text{CS}}$ is satisfied, the eavesdropper set $\mathcal{E}$ can decode the signal with high probability. Moreover, past decodings shall be accurate as well. In other words, the eavesdroppers may potentially act and perform as the legitimate system.

Grouping results so far, we can establish that the sensing phase of the proposed approach is Wolfowitz secret only when $E < K$. Note that this result has been obtained with the optimal decoder for the noiseless case (which is a conservative assumption and far from practical use), i.e. $\mathcal{P}0$. Note also that no other decoding strategy will be able to obtain K samples of a K-sparse vector from $E < K$ readings as far as every set of K columns of $\tilde{\mathbf{\Phi}}$ behaves like an orthonormal system according to the RIP [31]. As a corollary, the best that E eavesdroppers can do is to cooperate among them.

2) Eavesdroppers With Corrupted CSI: Let us assume now that the eavesdroppers have an imperfect knowledge of the wiretap sensing matrix $\tilde{\mathbf{\Phi}}$, modeled as

$$\hat{\mathbf{\Phi}} = \tilde{\mathbf{\Phi}} + \Sigma, \tag{22}$$

where $\hat{\mathbf{\Phi}}$ stands for the corrupted wiretap sensing matrix and $\Sigma \in \mathbb{R}^{E\times S}$ is a random matrix with i.i.d. Gaussian entries with zero mean and variance σ_Σ^2 that models the errors in the channel estimation. This perturbation in the sensing matrix results in a *multiplicative noise*, which is more difficult to analyze than the additive noise since it is correlated with the signal of interest [34].

Fortunately, recent works in the literature study similar problems [34], [35]. In particular, [35] analyzes the effect of a structured perturbation in the sensing matrix. It models $\hat{\mathbf{\Phi}}$ as

$$\hat{\mathbf{\Phi}} = \tilde{\mathbf{\Phi}} + \mathbf{B}\Delta \tag{23}$$

where $\mathbf{B} \in \mathbb{R}^{R\times S}$ is known a priori and Δ is a diagonal matrix of uniformly distributed and bounded entries. Focusing on small perturbations, i.e. $\|\Sigma\|/\|\tilde{\mathbf{\Phi}}\| < 1$ in our model, the authors show that an upper bound of the decoding error at the receiver grows linearly with the perturbation level. Therefore, it is meaningful to design strategies that corrupt the estimation of the wiretap channel at the eavesdroppers. This is the goal that will be pursued in Section V.

B. Eavesdropping During the Projection Phase

This phase is very robust against malicious and passive eavesdropping. Here, the derived results are not dependent on the number of eavesdroppers, since each eavesdropper in $\mathcal{E}$ has full access to the signal sent by the relays, i.e., $\mathbf{y}(n)$, to the fusion center (assuming that $\mathbf{y}(n)$ is not encrypted) as it is represented in Fig. 3.

This problem is similar to the key-based PHY-layer secrecy works in [20] and [21]. However, the main difference is that the sensing nodes do not encrypt the signal with any key. Instead, they send uncoded signals and the MAC implicitly performs random linear combinations modeled according to the matrices $\mathbf{\Phi}$ and $\tilde{\mathbf{\Phi}}$.

Actually, this key-less coding mechanism is not new and comes from the well-known discipline of Network Coding [36], 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 [37].

For Zero-Probability of Recovery, it is enough to proof that if the eavesdroppers try to reconstruct the signal with a wrong sensing matrix $\mathbf{\Phi}'$ (understanding 'wrong' as independent to $\mathbf{\Phi}$), the eavesdroppers will recover a R-sparse vector, instead of the K-sparse original one.

Lemma 3: Let $\mathbf{\Phi}$ and $\mathbf{\Phi}'$ be two $R \times S$ independent matrices following the Gaussian measurement ensemble. For a K-sparse vector $\mathbf{x}_K(n)$, let $\mathbf{y}(n) = \mathbf{\Phi}\mathbf{x}_K(n)$. Then, all $\hat{\mathbf{x}}_K(n)$ that satisfy $\mathbf{y}(n) = \Phi'\hat{\mathbf{x}}_K(n)$ are R-sparse with probability one.

Proof The proof is the same as the one in [20, Th. 1].

Remark 1: The main difference with [20] is that the authors obtained computational secrecy assuming a finite set of key matrices. Hence, an eavesdropper with unlimited computational power may sequentially test among all the possibilities until the recovered vector is K-sparse. Additionally, we can also ensure Zero-Probability of Recovery because the number of i.i.d. possible matrices is unbounded. Hence, the eavesdroppers have zero-probability to guess the correct one if no further information is provided.

In summary, ZPoR holds and this phase is secret in terms of Wolfowitz Secrecy.

V. Control of the CSI at the Eavesdroppers

Previous sections show that the AF-CS scheme offers a reasonable good protection against eavesdropping for relatively small groups of eavesdroppers, i.e., $E \leq K$. Although increasing this number of eavesdroppers to $E \sim K + K \log(S/K)$ in order to satisfy $\mathcal{C}_{\text{CS}}$ (and hence achieve high PoR), may become unpractical in most cases, we propose additional strategies that increases the PHY-layer secrecy. In what follows, we introduce two different techniques, both based on the fact that a corrupted estimation of the wiretap sensing matrix decreases the eavesdropping capabilities during the sensing phase. Therefore, these strategies ensure that the sensing matrix at the eavesdroppers cannot be estimated without error.

A. Pseudorandom Training Phase

One possible technique is to add a pseudorandom sequence $s(n) \sim \mathcal{N}(0, \sigma_s^2)$ to the training pilots of amplitude A. Hence, the pilot signal from sth sensing node at the rth relay is:

$$p_{r,s}(n) = (A + s(n))[\mathbf{\Phi}]_{r,s} + [\mathbf{w}(n)]_r. \tag{24}$$

On the other hand, the eth eavesdropper will receive the pilot signal from the sth sensing node as

$$p_{e,s}(n) = (A + s(n))[\tilde{\mathbf{\Phi}}]_{e,s} + [\tilde{\mathbf{w}}(n)]_e. \tag{25}$$

Note that we have assumed only partial knowledge of the pseudorandom pilot sequences at the eavesdroppers. More specifically, they may obtain the mean of the sequence, i.e. the value of A, but no knowledge is assumed about the statistical nature of $s(n)$. Furthermore, the channel state $[\mathbf{\Phi}]_{r,s}$ is assumed to be constant during the estimation process.

After N transmissions, the Maximum Likelihood Estimation (MLE) of $[\mathbf{\Phi}]_{r,s}$ for the intended nodes is well-known [38] and results in:

$$[\hat{\mathbf{\Phi}}]_{r,s} = \frac{\sum_{n=1}^{N} [\mathbf{p}]_n (A + s(n))}{\sum_{n=1}^{N} (A + s(n))^2}. \tag{26}$$

with an MSE of

$$\mathbb{E}\left[([\hat{\mathbf{\Phi}}]_{r,s} - [\mathbf{\Phi}]_{r,s})^2\right] = \frac{\sigma_{\mathbf{w}}^2}{N(A^2 + \sigma_s^2)}. \tag{27}$$

So the system may decrease the estimation error as much as desired by increasing the power of the pilots $A^2+\sigma_s^2$ and/or the number of pilots N (with the subsequent energy and signaling costs). Therefore, we assume perfect channel state information at the relays.

Similarly, the eavesdroppers can estimate the channel coefficient $[\tilde{\mathbf{\Phi}}]_{e,s}$ with the difference that we assume $s(n)$ only known by the intended nodes.

Since $s(n)$ is unknown by the eavesdroppers and treated as multiplicative noise, the resulting signal model at the eth eavesdropper is (for the sake of simplicity in the notation, let the N-dimensional vector $\mathbf{p}$ represent the collected N pilot samples $p_{e,s}(n)$, φ represent $[\hat{\mathbf{\Phi}}]_{e,s}$, $\hat{\varphi}$ represent $[\hat{\tilde{\mathbf{\Phi}}}]_{e,s}$ and $w(n)$ is $[\mathbf{w}(n)]_e$):

$$[\mathbf{p}]_n = (A + s(n))\varphi + w(n) = A\varphi + t(n), \tag{28}$$

where the term $A\varphi$ can be seen as the desired signal and $t(n) = \varphi s(n) + w(n)$ as the noise term with variance $\sigma_t^2 = |\varphi|^2\sigma_s^2 + \sigma_w^2$. The eavesdropper is unaware of the actual dependence between σ_t^2 and φ and hence it is not considered in the following derivation of the MLE of φ.

To actually find the MLE of φ, we first write the pdf of $\mathbf{p}$ as a function of φ as

$$f(\mathbf{p}; \varphi) = \frac{1}{(2\pi\sigma_t^2)^{\frac{N}{2}}} \exp\left[-\frac{1}{2\sigma_t^2}\sum_{n=1}^{N}([\mathbf{p}]_n - A\varphi)^2\right]. \tag{29}$$

The log-likelihood function of φ becomes

$$\ln f(\mathbf{p}; \varphi) = -\frac{N}{2}(2\pi\sigma_t^2) - \frac{1}{2\sigma_t^2}\sum_{n=1}^{N}([\mathbf{p}]_n - A\varphi)^2. \tag{30}$$

Taking its derivative we get

$$\frac{\partial \ln f(\mathbf{p}; \varphi)}{\partial \varphi} = -\frac{1}{2\sigma_t^2}\left(-2A\sum_{n=1}^{N}[\mathbf{p}]_n + 2NA^2\varphi\right). \tag{31}$$

Setting it equal to zero and solving for $\hat{\varphi}$ we obtain the MLE

$$\hat{\varphi} = \frac{\sum_{n=1}^{N}[\mathbf{p}]_n}{NA}, \tag{32}$$

where the MSE of the estimator $\hat{\varphi}$ is

$$\mathbb{E}\left[(\varphi - \hat{\varphi})^2\right] = \frac{|\varphi|^2\sigma_s^2 + \sigma_{\mathbf{w}}^2}{NA^2}. \tag{33}$$

Note that this is the MSE computed for one channel coefficient (i.e., the channel between sth sensing node and eth eavesdropper). The average MSE, i.e. $\widehat{\text{MSE}}$ for all the channel coefficients is computed as:

$$\widehat{\text{MSE}} = \frac{\mathbb{E}[|[\tilde{\mathbf{\Phi}}]_{e,s}|^2]\sigma_s^2 + \sigma_{\mathbf{w}}^2}{NA^2} = \frac{\sigma_s^2\sigma_{\mathbf{\Phi}}^2 + \sigma_{\mathbf{w}}^2}{NA^2}. \tag{34}$$

Clearly, the introduction of the pseudorandom sequence $s(n)$ achieves a double improvement. On the one hand, it reduces the channel estimation distortion at the intended nodes, which is an expected consequence since the system is spending more power in pilots. On the other hand, it introduces an additional error in the estimation of the eavesdroppers.

The reader may notice that we are assuming $s(n)$ to be known by the intended nodes but not by the eavesdroppers. In principle, this assumption may seem hard because it implies to send $s(n)$ securely using an alternative channel. In other words, it looks like a circular argument where in order to send information securely, it is assumed that some prior information (in this case $s(n)$) has been already sent securely.

However, many techniques have been reported in the literature that allow "off-air" synchronisation of pseudorandom sequences, e.g., in [18] these type of strategies are used to generate the same sensing matrix in a distributed way for the transmitters and the receiver, and in [20] the authors generate a random key that is known to the transmitter and the receiver but not to any intruder. Using these techniques, each sensor can locally generate a sequence $s(n)$ (which is different for each sensing node) in an efficient manner by using the same seed of a pseudorandom generator. This seed may be a function of the network identifier (or any other parameter related to the management of the network or to the hardware of the device) that is known a priori by the intended nodes and unknown by a potential eavesdropper. Hence, since there is no transmission over the air, the pseudorandom sequence is protected against eavesdropping.

B. Two-Way Secure Training Phase

Although the previous scheme is fully implementable as a PHY-layer secret training phase, let us also consider the case where the eavesdroppers have access to the initial configuration of the intended nodes, i.e, the seed and the pseudorandom generator, and can replicate $s(n)$. In such a case, they are able to decode the intended signal with high PoR if E satisfies $\mathcal{C}_{\text{CS}}$.

One possible way to overcome this problem is to exploit the reciprocity of the channel in order to design a *key-less* PHY-layer secret training phase. This approach has been studied in the literature [15]–[17] for MIMO scenarios. Based on these techniques, we propose a simplified adaptation for our single-antenna sensor case. The algorithm is based on a two-way estimation process that encompasses: i) a reverse training phase and ii) a forward training phase.

1) Reverse Training Phase: In this phase, the relay sends an uncoded pilot sequence of length N and amplitude A. The sth sensing node will receive $p_{s,r}(n) = A\phi_b + w(n)$, where ϕ_b denotes the backward channel coefficient that links sensors s and r and is approximately the same as $[\mathbf{\Phi}]_{r,s}$ when channel reciprocity holds. Moreover $w(n)$ is the AWGN of the channel. After N pilots, the sensing node can estimate ϕ_b as:

$$\hat{\phi}_b = \frac{1}{NA}\sum_{i=1}^{N} p_{s,r}(n) = \phi_b + \varepsilon_b, \tag{35}$$

where $\varepsilon_b \sim \mathcal{N}(0, \frac{\sigma^2}{NA})$ is the estimation error during the reverse training phase.

On the other hand the eavesdropper e will receive $p_{e,r}(n) = A\xi_b + w(n)$, where ξ_b denotes the channel coefficient from the relay r to e. However, note that this coefficient does not correspond to the sensor-eavesdropper coefficient, so it is not helpful in order to build the sensing matrix.

2) Forward Training Phase: The sensing node transmits to the relays the sequence $s = Af(\hat{\phi}_b)$, where $f(\hat{\phi}_b)$ is a bijective function of $\hat{\phi}_b$, e.g. $f(x) = 1 - \alpha/x$ with $x, \alpha \in \mathbb{R}$. The rth relay receives $q_{r,s} = Au + w(n)$, where u corresponds to $f(\hat{\phi}_b)\phi_f$, being ϕ_f the forward channel coefficient from sensor s to relay node r, i.e. $\phi_f = [\mathbf{\Phi}]_{r,s}$. After N' transmissions, the relay can obtain an estimation of u, that is

$$\hat{u} = \frac{1}{N'A}\sum_{i=1}^{N} q_{r,s}(n) = u + \varepsilon_f, \tag{36}$$

where $\varepsilon_f \sim \mathcal{N}(0, \frac{\sigma^2}{N'A})$ is the estimation error during the forward training phase. Then, the decoder can easily estimate $\hat{\phi}_f$ if it takes into account the function $f(x)$ and channel reciprocity, i.e. $\phi_b \approx \phi_f$. In the example above, simply adding α to $\hat{u}$ gives

$$\hat{\phi}_f = \hat{u} + \alpha = \phi_f + \alpha\left(1 - \frac{\phi_f}{\phi_b + \varepsilon_r}\right) + \varepsilon_f. \tag{37}$$

For sufficiently large N, N' the terms ε_r and ε_f tend to zero, hence $|\phi_f - \hat{\phi}_f| \to 0$, which guarantees a consistent estimation of the intended channel coefficient.

On the other hand, the eavesdropper will receive $q_{e,s} = Av + w(n)$, where $v = f(\hat{\phi}_b)\varphi_f$ being φ_f the channel coefficient between sth sensing node and eth eavesdropper, i.e. $\varphi_f = [\tilde{\mathbf{\Phi}}]_{e,s}$. After averaging over the N' pilots, it obtains

$$\hat{v} = f(\hat{\phi}_b)\varphi_f + \varepsilon_f. \tag{38}$$

Note that even knowing $f(x)$, the eavesdropper gets a corrupted channel estimation. Following the example with $f(x) = 1 - \alpha/x$, it would compute

$$\hat{\varphi}_f = \hat{v} + \alpha = \varphi_f + \alpha\left(1 - \frac{\varphi_f}{\hat{\phi}_b}\right) + \varepsilon_f. \tag{39}$$

TABLE I

SIMULATION PARAMETERS

Parameter	Value
Number of *fusion nodes*:	$F = 1$
Number of *sensing nodes*:	$S = 200$
Number of *active sensors*:	$K = 10$
Number of *relay nodes*:	$R = 60$
Number of *eavesdropping nodes*:	$E = [0, 110]$
Compressed Sensing Condition:	$\mathcal{C}_{\mathrm{CS}} : E > 40$

TABLE II

SUMMARY OF THEORETICAL RESULTS

		perfect CSI	**corrupted CSI**
Sensing Phase	$E < K$	ZPoR	ZPoR
	$K \leq E \leq \mathcal{C}_{\mathrm{CS}}$	Low PoR	Arbitrarily Low PoR
	$E > \mathcal{C}_{\mathrm{CS}}$	High PoR	Arbitrarily Low PoR
Projection Phase		ZPoR	

For N' sufficiently large, $\hat{v} + \alpha = \varphi_f + \alpha(1 - \varphi_f/\hat{\phi}_b)$, and the channel estimation is corrupted in this case by the term $\alpha(1 - \varphi_f/\hat{\phi}_b)$.

Note that according to the design of $f(\hat{\phi}_b)$ the system may experiment different trade-offs between the total power spent during the training phase and the channel estimation distortion at the eavesdroppers. Although a complete analysis of the different functions that can be employed and their particular trade-off is out of the scope of the paper, we analyze the impact of the channel estimation distortion at the eavesdroppers in front of the obtained Probability of Recovery and wiretap distortion in Section VI.

Finally, note that in general the PoR can be made arbitrarily small at the expenses of transmitted power and therefore, the system is ideally secret in terms of Wolfowitz Secrecy.

VI. NUMERICAL RESULTS

In this section, we first summarize the theoretical results obtained in Section IV. Then, we evaluate the PHY-layer secrecy performance of the AF-CS scheme.

Table I summarizes the parameters that we consider in our simulations, where a star-topology network is considered. Besides, sensor readings are generated with an auto-regressive model of order 1 ($AR-1$) to emulate real sources [39]. The sth sensor reading is

$$x_s(n) = \rho x_s(n-1) + z(n), \quad \text{for } n = 1, 2, \ldots, \tag{40}$$

where $\rho \in [0, 1]$ is the auto-regression coefficient and assumed constant. The random process $z(n)$ is a sequence of Gaussian distributed and independent random variables with zero mean and variance σ_z^2. In our simulations, $\sigma_{x_s}^2$ is set to 1.

A. Summary of the Theoretical Results

Table II summarizes the PHY-secrecy performance for each of the possible cases. We have divided the analysis of the sensing phase in three cases depending on the number of eavesdroppers.

For low values of E (i.e., $E < K$), Zero-Probability of Recovery (ZPoR) can be guaranteed even in the case that the eavesdroppers have perfect channel estimation. For the

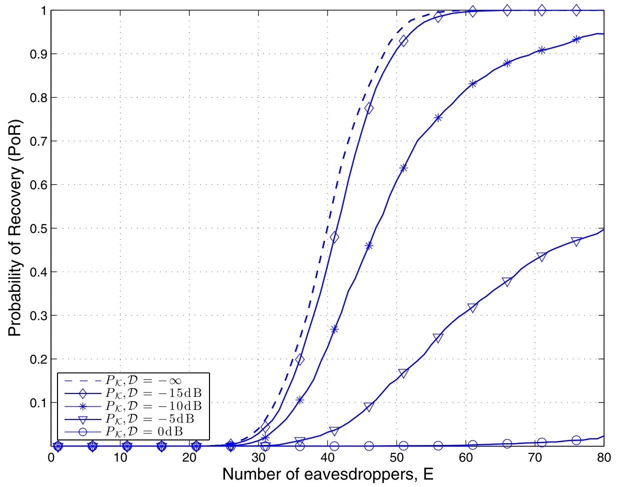

Fig. 5. Probability of Recovery as a function of the number of eavesdroppers and for different values of channel estimation distortion. This figure has been averaged over 1000 realizations.

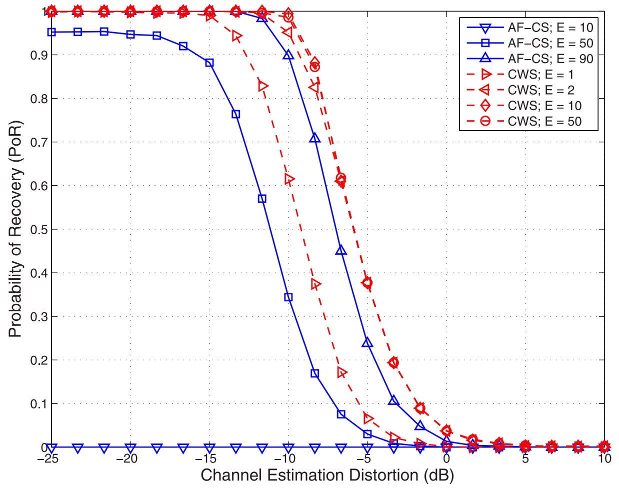

Fig. 6. Probability of Recovery as a function of the channel estimation distortion for different number of coordinated eavesdroppers for $K = 10$ and $S = 200$. Solid lines represent the performance of AF-CS while dashed lines denote CWS. This figure has been averaged over 1000 realizations.

particular case $E = K$, the *Probability of Recovery* (PoR) is asymptotically zero in S.

For moderate values of E (i.e., $K < E \leq \mathcal{C}_{\mathrm{CS}}$), the eavesdroppers cannot recover $\mathbf{x}_K(n)$ with high probability getting high wiretap distortion. However, Zero-Probability of Recovery cannot be guaranteed for that configuration.

Only for high values of E (i.e., $E > \mathcal{C}_{\mathrm{CS}}$) and with perfect CSI, the eavesdroppers can decode the signal $\mathbf{x}_K(n)$ with high probability. However, thanks to the introduction of the pseudorandom pilots technique, the intended nodes can corrupt the CSI of the eavesdroppers and make the wiretap distortion grow linearly with the introduced noise power. In the limit, Wolfowitz Secrecy is achieved.

The projection phase achieves Zero-Probability of Recovery in any case.

B. Probability of Recovery as a Function of the Number of Eavesdroppers

The numerical simulation has been run in Matlab as follows. For each realization, a new wiretap sensing matrix $\tilde{\mathbf{\Phi}}$ of dimension $E \times S$ has been randomly generated following a Gaussian measurement ensemble $\mathcal{N}(0, E^{-1})$. Next, for each channel distortion value $\mathcal{D}$, a perturbation matrix Σ has been generated as $\mathcal{N}(0, \sigma_{\Sigma}^2)$. The K nonzero entries of a random vector $\mathbf{x}_K(n)$ of sparsity K are distributed as $\mathcal{N}(0, \sigma_{\mathbf{x}}^2)$ and uniformly located across the S possible positions. Finally, the decoder $\mathcal{P}2$ has been implemented using CVX, a package for specifying and solving convex programs [40], [41].

In Fig. 5 we plot the Probability of Recovery (PoR) in terms of the number of eavesdroppers E. For perfect CSI at the eavesdroppers, the simulation supports that for small $E < K$, the recovery is infeasible, getting a PoR of 0. Moreover, for moderate values of E, i.e., $K < E < \mathcal{C}_{\mathrm{CS}}$ the signal is recovered with low probability. On the other hand, for values of E similar or greater than $\mathcal{C}_{\mathrm{CS}}$, the eavesdropping set can recover $\mathcal{K}(n)$ with high probability following the $\mathcal{C}_{\mathrm{CS}}$ condition. According to Fig. 5, we observe that the bound $\mathcal{C}_{\mathrm{CS}}$ (i.e., $E = 40$) divides the low and high PoR for values smaller and bigger than 0.5, respectively.

For corrupted CSI at the eavesdroppers, the simulation shows how the PoR is degraded. Even for small values of $\mathcal{D}$, e.g. $\mathcal{D} = -10$dB, the PoR degenerates drastically and values of PoR close to 1 can only be achieved for very large values of E ($E > 80$ nodes). For values of $\mathcal{D} = 0$dB (which means that the introduced perturbation is of the order of channel variance), the signal can be recovered with negligible probability.

C. Probability of Recovery Compared to CWS-Like Techniques

Next, we compare the AF-CS with CWS-like methods [18]. Both methods are CS-based distributed schemes. Although CWS has not been designed from a PHY-layer secure perspective, we assess its secrecy performance since its approach is one of the most extended CS schemes in WSN literature.

In Fig. 6, simulation results compare the performance of both AF-CS and CWS in front of a certain number of eavesdroppers. Using AF-CS, we notice that for $E < 10$, the eavesdroppers cannot recover the signal even when they have a perfect channel estimation. In fact, AF-CS requires the set of eavesdroppers to be higher than 50 in order to achieve a PoR close to 1 in some cases. On the other hand, the performance of CWS is lower since it can be observed that even for $E = 1$ the eavesdropper succeeds in decoding the signal (a PoR close to 1) with a channel distortion of less than -15dB. The reason of such a big difference is that the AF-CS exploits the security that gives the spatial diversity introduced by the relays. Hence, while in AF-CS scheme the projections are computed simultaneously at the relays, the CWS strategy computes them in different time slots. Therefore, one single eavesdropper can be listening and computing all the projections, i.e., acting like a fusion center.

Furthermore, Fig. 6 also shows the PoR results as a function of the channel estimation distortion $\mathcal{D}$. For very small distortion values (i.e, $\mathcal{D} < -20$dB) the performance drop is negligible. However, it degrades fast for values of $\mathcal{D} > -15$dB. For the case of $\mathcal{D} = 0$dB, the Probability of Recovery is negligible for any configuration.

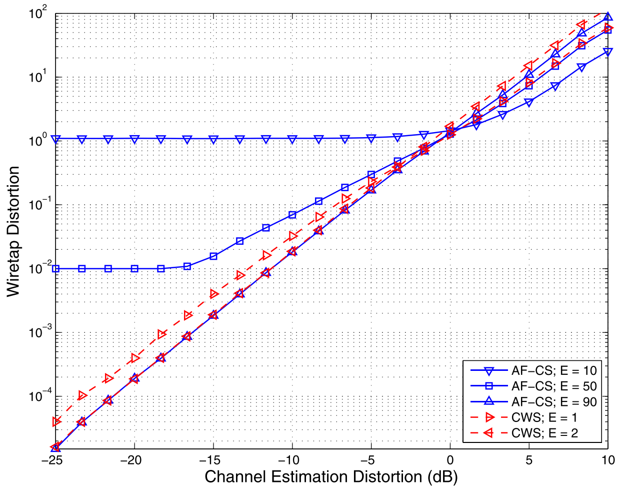

Fig. 7. Wiretap distortion as a function of the channel estimation distortion for different number of coordinated eavesdroppers for $K = 10$ and $S = 200$. Solid lines represent the performance of AF-CS while dashed lines denote CWS. This figure has been averaged over 1000 realizations.

In summary, results in Figs. 5 and 6 confirm that the PoR is always zero for $E < 10$ and that it can be made arbitrarily small for $E \geq 10$ at the expense of increasing the fraction of transmitted power devoted to corrupt the CSI at the eavesdroppers. In all these cases, Wolfowitz secrecy is guaranteed.

D. Wiretap Distortion as a Function of the Estimation Channel Distortion

Here we study the performance of the relative wiretap distortion as a function of the channel estimation distortion. This study actually extends the one in [34] and confirms some of their results. Mainly, we show (as in [34]) that the distortion at the receiver grows linearly with the power of the channel estimation distortion for values $\mathcal{D} < 0$dB. This is true (up to some error floor) not only for the case $\mathcal{D} < 0$dB but also when $\mathcal{D} > 0$dB, as we can see graphically in Fig. 7.

We also show that the relative wiretap distortion decreases for lower values of $\mathcal{D}$ up to some error floor, which is dependent on the number of eavesdroppers. It means that even for the ideal case of $\mathcal{D} = -\infty$dB, the relative wiretap distortion cannot be decreased further than the error floor.

However, probably the most relevant result of this subsection is the following: for values of $\mathcal{D} = 0$dB all the configurations achieve a similar wiretap distortion of 1. It means that the distortion of the reconstruction phase at the eavesdroppers is equal to the variance of the signal. That is to say, the eavesdroppers do not know anything about the signal $\mathbf{x}_K(n)$ as it can be appreciated in the following example.

Example 1: A given decoder that does not receive $y(n)$ and does not have any further information about $\mathbf{x}_K(n)$ than their entries are zero mean can guess $\hat{\mathbf{x}}_K(n) = \mathbf{0}$ and the wiretap distortion is

$$\mathcal{D}_e = \mathbb{E}\left[\frac{\|\mathbf{x}_K(n) - \mathbf{0}\|^2}{\|\mathbf{x}_K(n)\|^2}\right] = 1, \tag{41}$$

Hence, an important conclusion is that if the intended nodes set $\mathcal{D} = 0$dB, the eavesdroppers will achieve a wiretap distortion of 1 independently of E.

VII. Conclusion

In this paper, we have evaluated the Amplify-and-Forward Compressed Sensing (AF-CS) scheme as a physical layer secrecy solution for Wireless Sensor Networks (WSNs). In particular, we have studied its secrecy performance in each phase of the proposed framework against a passive eavesdropper agent composed by several malicious and coordinated nodes.

We have analytically demonstrated that AF-CS achieves Zero-Probability of Recovery for the cases when the number of eavesdroppers E is less than the sparsity level of the signal K. For a larger number of eavesdroppers, we have proposed two secure training phase strategies that contaminate their channel estimations. In fact, the wiretap distortion at the eavesdroppers grows linearly with the power of the introduced perturbation.

The simulation results support our claim that the scheme under study presents Zero-Probability of Recovery when the number of eavesdropping nodes is less than the sparsity level of the signal. On the other hand, and assuming the ideal case of perfect channel estimation at the eavesdropper's side, high decoding rates (higher than 0.5) are only achievable when the number of eavesdropping nodes is high enough to satisfy the restricted isometric property condition. Moreover, we show that the required number of eavesdroppers increases fast as a function of their channel estimation degradation and therefore the system can adapt the level of induced distortion in order to control the Probability of Recovery of the eavesdroppers. Actually, we have observed that for channel perturbations similar to the channel variance, the eavesdroppers obtain the same wiretap distortion as almost without any knowledge about the signal. However, the price to pay is that the more distortion we add at the eavesdroppers, the higher the energy cost at the sensing nodes. Furthermore, AF-CS drastically outperforms other distributed compressed sensing solutions for WSNs in terms of physical layer secrecy.

References

[1] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," in *Proc. IEEE Int. Conf. Commun.*, vol. 1, Jun. 2004, pp. 458–462.

[2] S. Shafiee and S. Ulukus, "Capacity of multiple access channels with correlated jamming," in *Proc. IEEE Military Commun. Conf.*, vol. 1, Oct. 2005, pp. 218–224.

[3] M. Srivatsa, "Who is listening? Security in wireless networks," in *Proc. Int. Conf. Signal Process., Commun. Netw.*, Jan. 2008, pp. 167–172.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[7] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[8] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE ISIT*, Nice, France, Jul. 2007, pp. 1296–1300.

[9] L. Zhang, R. Zhang, Y. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.

[10] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE 62nd VTC*, vol. 3. Sep. 2005, pp. 1906–1910.

[11] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[12] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Trans. Wireless Commun.*, to be published.

[13] 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 Eur. Signal Process. Conf.*, Barcelona, Spain, Aug. 2011, pp. 363–367.

[14] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as an energy-efficient solution for wireless sensor networks," *IEEE Sensors J.*, 2013, to be published.

[15] T.-H. Chang, W.-C. Chiang, Y. P. Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 6223–6237, Dec. 2010.

[16] X. Zhou, T. A. Lamahewa, P. Sadeghi, and S. Durrani, "Two-way training: Optimal power allocation for pilot and data transmission," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 564–569, Feb. 2010.

[17] C.-W. Huang, T.-H. Chang, X. Zhou, and Y.-W. P. Hong, "Two-way training for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2724–2738, May 2013.

[18] W. Bajwa, J. Haupt, A. Sayeed, and R. Nowak, "Compressive wireless sensing," in *Proc. 5th Int. Conf. IPSN*, New York, NY, USA, Apr. 2006, pp. 134 –142.

[19] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[20] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 813–817.

[21] M. R. Mayiami, B. Seyfe, and H. G. Bafghi, "Perfect secrecy using compressed sensing," *CoRR*, vol. abs/1011.3985, 2010.

[22] S. Agrawal and S. Vishwanath, "Secrecy using compressive sensing," in *Proc. IEEE ITW*, Oct. 2011, pp. 563–567.

[23] G. Reeves, N. Goela, N. Milosavljevic, and M. Gastpar, "A compressed sensing wire-tap channel," in *Proc. IEEE ITW*, Oct. 2011, pp. 548–552.

[24] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[25] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT*, Jun. 2007, pp. 2466–2470.

[26] H. S. Anderson, "On discovering the compressive sensing matrix from few signal/measurement pairs," in *Proc. IEEE WIFS*, 2011.

[27] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.

[28] E. Candès, "The restricted isometry property and its implications for compressed sensing," *Comp. Rendus Math.*, vol. 346, nos. 9–10, pp. 589–592, 2008.

[29] N. Marina, H. Yagi, and H. V. Poor, "Improved rate-equivocation regions for secure cooperative communication," in *Proc. IEEE ISIT*, Aug. 2011, pp. 2871–2875.

[30] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE ISIT*, Jul. 2008, pp. 524–528.

[31] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[32] E. J. Candès and Y. Plan, "A probabilistic and RIPless theory of compressed sensing," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7235–7254, Nov. 2011.

[33] X. Feng and Z. Zhang, "The rank of a random matrix," *Appl. Math. Comput.*, vol. 185, no. 1, pp. 689–694, 2007.

[34] M. A. Herman and T. Strohmer, "General deviants: An analysis of perturbations in compressed sensing," *IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 2, pp. 342–349, Apr. 2010.

[35] Z. Yang, C. Zhang, and L. Xie, "Robustly stable signal recovery in compressed sensing with structured matrix perturbation," *IEEE Trans. Signal Process.*, vol. 60, no. 9, pp. 4658–4671, Sep. 2012.

[36] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Network Coding Theory*. Norwell, MA, USA: Now Publishers, 2005.

[37] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*. Norwell, MA, USA: Now Publishers, 2007.

[38] S. M. Kay, *Fundamentals of Statistical Signal Processing, Estimation Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.

[39] T. Hashimoto and S. Arimoto, "On the rate-distortion function for the nonstationary Gaussian autoregressive process," *IEEE Trans. Inf. Theory*, vol. 26, no. 4, pp. 478–480, Jul. 1980.

[40] M. Grant and S. Boyd, *CVX: Matlab Software for Disciplined Convex Programming*. Austin, TX, USA: CVX Res. Inc., Apr. 2011.

[41] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control* (Lecture Notes in Control and Information Sciences), V. Blondel, S. Boyd, and H. Kimura, Eds. New York, NY, USA: Springer-Verlag, 2008, pp. 95–110.

Joan Enric Barceló-Lladó received the M.Sc. degree in electrical engineering and the Ph.D. degree from the Universitat Autònoma de Barcelona (UAB), Spain, in 2007 and 2012, respectively.

In 2007, he was a Research Assistant with the Università degli Studi di Siena, Italy, involved in the topics of cross-layer techniques for satellite networks. From 2008 to 2009, he held a visiting position with the Universitetsstudiene på Kjeller-University Graduate Center, Oslo, Norway, where he was involved in resource allocation for satellite communications based on game theory. He was with the Signal Processing for Communications and Navigation Group, Department of Telecommunication and Systems Engineering, UAB, in 2009. He was involved in several national and international projects with public and private fundings. His current areas of interest are related to algorithms for energy-efficient communications with correlated sources in wireless sensor networks.

Antoni Morell received the M.Sc. degree in electrical engineering and the Ph.D. degree from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 2002 and 2008, respectively.

He was with the Signal Theory and Communications Department, UPC, from 2002 to 2005. He was with the Universitat Autònoma de Barcelona, as a Research and Teaching Assistant in 2005, and later as an Assistant Professor in 2008, teaching courses on communications, signals, and systems. He has been involved in more than 10 research and development projects, national and international projects, being the Principal Investigator in one of them. He has expertise in optimization techniques applied to communications, also in the field of wireless sensor networks. He has authored more than 30 papers in recognized international journals and conference proceedings. His current research interests include distributed multiple access protocols, distributed source coding, compressed sensing, routing strategies in WSNs, and inertial-aided indoor positioning.

Gonzalo Seco-Granados (S'97–M'02–SM'08) received the Ph.D. degree in telecommunication engineering from the Universitat Politècnica de Catalunya, Barcelona, Spain, and the M.B.A. degree from the Instituto de Estudios Superiores de la Empresa-University of Navarra, Barcelona, in 2000 and 2002, respectively.

From 2002 to 2005, he was a member of the technical staff with the RF Payload Division, European Space Research and Technology Center, European Space Agency, Noordwijk, The Netherlands, where he was involved in the Galileo project. He led the activities concerning navigation receivers and indoor positioning for GPS and Galileo. Since 2006, he has been an Associate Professor with the Department of Telecommunications and Systems Engineering, Universitat Autònoma de Barcelona (UAB), Barcelona. From 2007 to 2011, he was a coordinator of the Telecommunications Engineering degree. Since 2011, he has been the Vice Director with the UAB Engineering School. In 2008, he was a Director of one of the six Chairs of Technology and Knowledge Transfer UAB Research Park Santander.

Dr. Seco-Granados has been a Principal Investigator of 20 National and International Research projects, and an Advisor of the European Commission in topics related to communications and navigation. He has had several visiting appointments with Brigham Young University and the University of California at Irvine. He has authored more than 30 journal papers and 110 conference contributions, and holds two patents under exploitation. His research interests include signal processing for wireless communications and navigation, estimation theory, synchronization, location-based communications, and optimization.